625-CD-017-001

EOSDIS Core System Project

ECS Training Material Volume 17: System Troubleshooting

December 1997

Hughes Information Technology Systems
Upper Marlboro, Maryland

ECS Project Training Material
Volume 17: System Troubleshooting

December 1997

Prepared Under Contract NAS5-60000
CDRL Item 129

RESPONSIBLE ENGINEER

Paul E. Van Hemel /s/ 12/19/97

Paul E. Van Hemel Date
EOSDIS Core System Project

SUBMITTED BY

Thomas Hickey /s/ 12/19/97

Tom Hickey, M&O Manager Date
EOSDIS Core System Project

Hughes Information Technology Systems
Upper Marlboro, Maryland

This page intentionally left blank.

Preface

This document is a contract deliverable with an approval code of 3. As such, it does not require formal Government approval. This document is delivered for information only, but is subject to approval as meeting contractual requirements.

Any questions should be addressed to:

Data Management Office
The ECS Project Office
Hughes Information Technology Systems
1616 McCormick Drive
Upper Marlboro, MD 20774-5372

This page intentionally left blank.

Abstract

This is Volume 17 of a series of lessons containing the training material for Version 2 Drop 2 of the Earth Observing System Data and Information System (EOSDIS) Core System (ECS). This lesson provides a detailed description of the different tasks that are required to perform system troubleshooting. The lesson includes a detailed review of the system monitoring capabilities, hardware and software troubleshooting process, and trouble ticket set-up and processing.

***Keywords**:* training, instructional design, course objective, system troubleshooting, trouble ticket, maintenance

This page intentionally left blank.

Change Information Page

List of Effective Pages	
Page Number	**Issue**
Title	Original
iii through xii	Original
1 through 70	Original
Slide Presentation 1 through 53	Original

Document History			
Document Number	**Status/Issue**	**Publication Date**	**CCR Number**
625-CD-017-001	Original	December 1997	

This page intentionally left blank.

Contents

Preface

Abstract

Introduction

Related Documentation

System Troubleshooting Overview

System Performance Monitoring

Problem Analysis/Troubleshooting

Troubleshooting of Custom Software

Trouble Ticket (TT)

Diagnosing Network Communications Problems

Practical Exercise

Slide Presentation

This page intentionally left blank.

Introduction

Identification

Training Material Volume 17 is part of Contract Data Requirements List (CDRL) Item 129, whose requirements are specified in Data Item Description (DID) 625/OP3 and is a required deliverable under the Earth Observing System Data and Information System (EOSDIS) Core System (ECS), Contract (NAS5-6000).

Scope

Training Material Volume 17 describes the process and procedures for ECS System Troubleshooting. This lesson is designed to provide the operations staff with sufficient knowledge and information to satisfy all lesson objectives.

Purpose

The purpose of this Student Guide is to provide a detailed course of instruction that forms the basis for understanding System Troubleshooting   Lesson objectives are developed and will be used to guide the flow of instruction for this lesson. The lesson objectives will serve as the basis for verifying that all lesson topics are contained within this Student Guide and slide presentation material.

Status and Schedule

This lesson module provides detailed information about training for Version 2.0, Drop 2. Subsequent revisions will be submitted as needed.

Organization

This document is organized as follows:

Introduction:	The Introduction presents the document identification, scope, purpose, and organization.
Related Documentation:	Related Documentation identifies parent, applicable and information documents associated with this document.
Student Guide:	The Student Guide identifies the core elements of this lesson. All Lesson Objectives and associated topics are included.
Slide Presentation:	Slide Presentation is reserved for all slides used by the instructor during the presentation of this lesson.

This page intentionally left blank.

Related Documentation

Parent Document

The parent document is the document from which this ECS Training Material's scope and content are derived.

423-41-01	Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work

Applicable Documents

The following documents are referenced within this ECS Training Material, or are directly applicable, or contain policies or other directive matters that are binding upon the content of this document:

420-05-03	Goddard Space Flight Center, Earth Observing System (EOS) Performance Assurance Requirements for the EOSDIS Core System (ECS)
423-41-02	Goddard Space Flight Center, Functional and Performance Requirements Specification for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS)

Information Documents

Information Documents Referenced

The following documents are referenced herein and amplify or clarify the information presented in this document. These documents are not binding on the content of the ECS Training Material.

535-TIP-CPT-001	Goddard Space Flight Center, Mission Operations and Data Systems Directorate (MO&DSD) Technical Information Program Networks Technical Training Facility, Contractor-Provided Training Specification
609-CD-003-001	Operations Tools Manual for the ECS Project
611-CD-004-001	Mission Operations Procedures for the ECS Project

Information Documents Not Referenced

The following documents, although not referenced herein and/or not directly applicable, do amplify or clarify the information presented in this document. These documents are not binding on the content of the ECS Training Material.

220-TP-001-001	Operations Scenarios - ECS Release B.0 Impacts, Technical Paper for the ECS Project
305-CD-020-002	Release B SDPS/CSMS System Design Specification Overview for the ECS Project
305-CD-021-002	Release B SDPS Client Subsystem Design Specification for the ECS Project
305-CD-022-002	Release B SDPS Interoperability Subsystem Design Specification for the ECS Project
305-CD-023-002	Release B SDPS Data Management Subsystem Design Specification for the ECS Project
305-CD-024-002	Release B SDPS Data Server Subsystem Design Specification for the ECS Project
305-CD-025-002	Release B SDPS Ingest Subsystem Design Specification [for the ECS Project
305-CD-026-002	Release B SDPS Planning Subsystem Design Specification for the ECS Project
305-CD-027-002	Release B SDPS Data Processing Subsystem Design Specification for the ECS Project
305-CD-028-002	Release B CSMS Communications Subsystem Design Specification for the ECS Project
305-CD-029-002	Release B CSMS System Management Subsystem Design Specification for the ECS Project
305-CD-030-002	Release B GSFC DAAC Design Specification for the ECS Project
305-CD-031-002	Release B Langley DAAC Design Specification for the ECS Project
305-CD-033-002	Release B EDC DAAC Design Specification for the ECS Project
305-CD-034-002	Release B ASF DAAC Design Specification for the ECS Project
305-CD-035-002	Release B NSIDC DAAC Design Specification for the ECS Project
305-CD-036-002	Release B JPL PO.DAAC Design Specification for the ECS Project
305-CD-037-002	Release B ORNL DAAC Design Specification for the ECS Project

305-CD-038-002	Release B System Monitoring and Coordination Center Design Specification for the ECS Project
305-CD-039-002	Release B Data Dictionary Subsystem Design Specification for the ECS Project
601-CD-001-004	Maintenance and Operations Management Plan for the ECS Project
604-CD-001-004	Operations Concept for the ECS Project: Part 1-- ECS Overview
604-CD-002-003	Operations Concept for the ECS Project: Part 2B -- ECS Release B
605-CD-002-001	Release B SDPS/CSMS Operations Scenarios for the ECS Project
607-CD-001-002	ECS Maintenance and Operations Position Descriptions
500-1002	Goddard Space Flight Center, Network and Mission Operations Support (NMOS) Certification Program, 1/90

This page intentionally left blank.

System Troubleshooting Overview

Lesson Overview

This lesson will provide you with the process for system/performance monitoring, problem analysis and troubleshooting of system hardware and software, managing the trouble ticket system, and diagnosing network communications problems. It provides practical experience in using the tools you will need for resolving system problems and minimizing system down time.

Lesson Objectives

Overall Objective - The overall objective of this lesson is proficiency in the methodology and procedures for system troubleshooting of the Earth Observing System Data and Information System (EOSDIS) Core System (ECS).

Condition - The student will be given a workstation console with access to ECS software tools including Trouble Ticket, Fault/Performance Management, HP OpenView, and Management Services Subsystem (MSS) graphical user interface (GUI) tools.

Standard - The student will use the tools in accordance with prescribed methods and complete required procedures without error.

Specific Objective 1 - The student will conduct system performance monitoring, to include checking the health and status of the network and accessing the EOSDIS Backbone Network (EBnet) Web Page.

Condition - The student will be given a workstation console with access to HP OpenView.

Standard - The student will use HP OpenView in accordance with specified procedures and without error to examine maps for color alerts and new nodes, create special submaps for monitoring status, and check for event notifications.

Specific Objective 2 - The student will perform problem analysis and troubleshooting, to include analysis and troubleshooting of the system, analysis and troubleshooting of commercial off-the-shelf (COTS) hardware, and COTS and custom software.

Condition - The student will be given a workstation console with access to ECS software tools including Trouble Ticket, Fault/Performance Management, HP OpenView, and Management Services Subsystem (MSS) graphical user interface (GUI) tools.

Standard - The student will use the GUI tools without error in accordance with applicable procedures to perform the required troubleshooting and maintenance activities.

Specific Objective 3 - The student will perform the functions required to set up and manage trouble ticket processing, including administrative set-up of user accounts and privileges in the trouble ticket software.

Condition - The student will be given a workstation console with access to ECS software tools including Trouble Ticket, Fault/Performance Management, HP OpenView, and Management Services Subsystem (MSS) graphical user interface (GUI) tools.

Standard - The student will use the GUI tools without error in accordance with applicable procedures to perform the required trouble ticket functions.

Specific Objective 4 - The student will perform the functions required to diagnose network communications problems.

Condition - The student will be given a workstation console with access to ECS software tools including Fault/Performance Management, HP OpenView, and Management Services Subsystem (MSS) graphical user interface (GUI) tools.

Standard - The student will use the GUI tools without error in accordance with applicable procedures to perform the required troubleshooting/diagnosis of network communications problems.

Importance

This lesson provides students with the knowledge and skills needed for effective system troubleshooting and maintenance of the ECS. It is structured to provide useful skills and knowledge concerning ECS operation and the tools for identifying system problems and returning malfunctioning system hardware and software to normal operational status. It provides useful instruction and practical exercises in maintaining ECS in an operationally ready condition, and is therefore vital to students who are preparing for a number of different positions with responsibilities in maintaining that system readiness, including positions as:

- Computer Operator, System Administrator, and Maintenance Coordinator at the DAAC.
- System Engineer, System Test Engineer, System Administrator, and Software Maintenance Engineer at the Sustaining Engineering Organization (SEO).
- System Engineer, System Test Engineer, and Software Maintenance Engineer at the DAAC.

System Performance Monitoring

The key to maintaining ECS in an operationally ready state is effective performance monitoring.

- System operators – close monitoring of progress and status of system and subsystem functions that are the focus of their jobs.
  - Notice any serious degradation of system performance that has an impact on their abilities to conduct their jobs successfully and meet user needs.
- System administrators and system maintenance personnel – monitor overall system functions and performance.
  - Administrative and maintenance oversight of system.
  - Watch for system problem alerts.
  - Use monitoring tools to create special monitoring capabilities.
  - Check for notification of system events.

Checking the Health and Status of the Network

ECS is heavily dependent on the use of computer networks. HP OpenView is a management tool that provides operators and maintainers with a system view for monitoring and checking the network, for quickly identifying parts of the network that may have problems, and for isolating faults on the network. It provides the following general features:

- a site-wide view of network and system resources.
- status information on resources.
- event notifications and background information.
- operator interface for managing resources.

Specific monitoring capabilities provided by HP OpenView Network Node Manager (NNM) include:

- a network map with color alerts to indicate problems.
- indication of network changes.
- creation of submaps for special monitoring.
- event notifications.

Figure 1 shows an example of network map screens from HP OpenView.

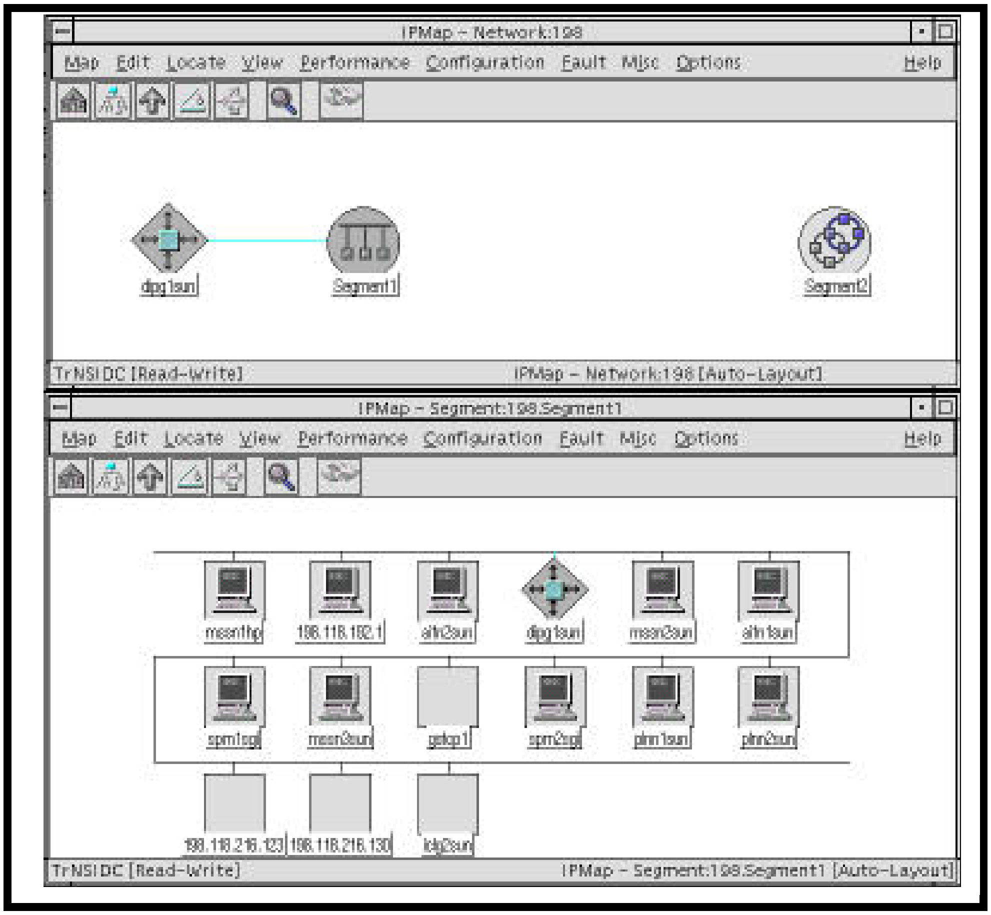

IPMap - Network:198
Map Edit Locate View Performance Configuration Fault Misc Options Help
dipg1sun
Segment1
Segment2
TrNSIDC [Read-Write]
IPMap - Network:198 [Auto-Layout]
IPMap - Segment:198.Segment1
Map Edit Locate View Performance Configuration Fault Misc Options Help
mssn1hp
198.118.192.1
aitn2sun
dipg1sun
mssn2sun
aitn1sun
spm1sgi
mssn3sun
gstcp1
spm2sgi
plnn1sun
plnn2sun
198.118.216.123
198.118.216.130
icig2sun
TrNSIDC [Read-Write]
IPMap - Segment:198.Segment1 [Auto-Layout]

Figure 1. Example of Network Map Screens from HP OpenView

HP OpenView is capable of discovering a network and its elements. To use HP OpenView NNM to monitor the network, it must be running and configured to display status, with its Network map set for read-write and the Internet Protocol (IP) map enabled.

Starting and Ending a NNM Session

For NNM to report properly on the network topography, HP OpenView Windows (OVW) must be activated. Once activated, OVW automatically starts NNM, as well as any installed and registered NNM applications. As a prerequisite, the network management processes that work with OVW and NNM must be running. These network management processes are:

- **ovwdb** - the process that maintains the OVW database.
- **trapd** - the process that multiplexes and logs SNMP traps.
- **ovtopmd** - the process that maintains the network topology database.

- **ovactiond** - the process that executes commands upon receipt of an event.
- **snmpCollect** - the process that collects MIB data and performs threshold monitoring.
- **netmon -** the process that polls SNMP agents for initial discovery of the network topology and for detecting changes in the network topology, configuration, and status.

To see if these processes are running, type **/usr/OV/bin/ovstatus** at a UNIX prompt on the HP OpenView server.

To perform the start-up, use the following procedure.

Start the HP OpenView Windows NNM Graphical User Interface

1 On workstation ***x*0msh*##***, at the UNIX prompt in a terminal window, type **/usr/OV/bin/ovstatus** at a UNIX command prompt and then press the **Return** key.

- NOTE: The ***x*** in the workstation name will be a letter designating your site: **g** = GSFC, **m** = SMC, **l** = LaRC, **e** = EDC, **n** = NSIDC, **o** = ORNL, **a** = ASF, **j** = JPL; the ***##*** will be an identifying two-digit number (e.g., **G0MSH08** indicates a management services subsystem *hp* workstation at GSFC). If you access the workstation through a remote login (rlogin), you must enter **xhost +** prior to the rlogin, and enter **setenv DISPLAY <local_workstation IP address>:0.0** after the rlogin before entering the **ovstatus** command.
- A series of messages is displayed indicating for each process that its state is “**RUNNING**” or “**NOT_RUNNING**.”
- If the network management processes are not running, a system administrator (logged in as **root**) can start them by typing **/usr/OV/bin/ovstart** and then pressing the **Return** key.

2 Type **/usr/OV/bin/ovw &** and press the **Return** key.

- The **About OVW** box is displayed, followed in a few moments by the OVW submap window, and any installed and registered NNM applications are also started.
- The **Event Categories** window is displayed in the upper right corner of the screen.

To exit NNM and all other integrated applications, use the following procedure.

Exit NNM

1 From the menu bar on any submap window, follow menu path **Map→Exit**.

[or]

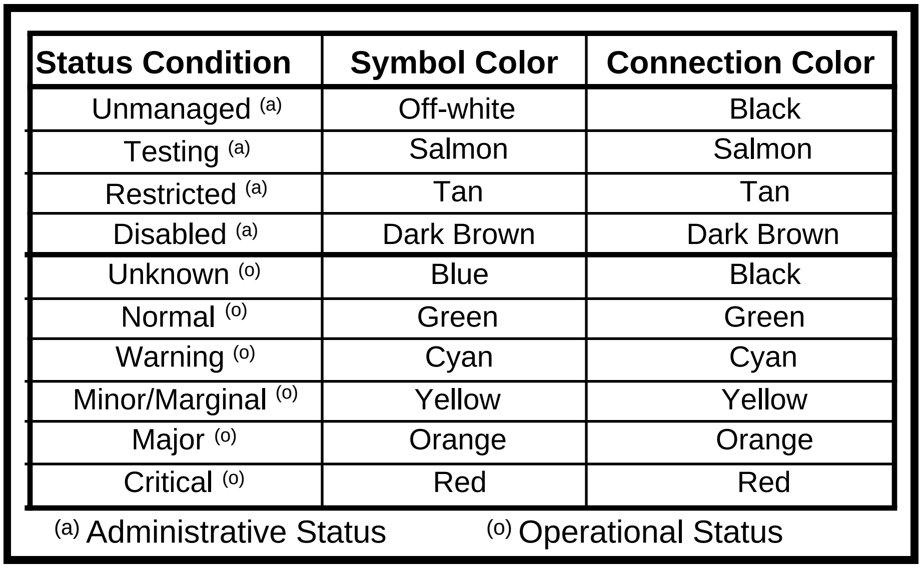
2 Click on the **Close** button on all open submap windows until the **Root** window is displayed. Then click on the **Close** button ( ) on the **Root** window.

- The open map is saved and all submap windows and dialog boxes of the map are closed. OVW, all NNM applications, and all other integrated applications exit.

If you are logged in with HP OpenView NNM running you can get a quick assessment of the health and status of the network by checking the network map for color alerts. The symbols and the connections between them on the network map are color-coded to indicate status. There are two status categories:

- administrative – not propagated from child to parent through the network.
- operational – propagated from child to parent to indicate problems.

If the compound status (how status is propagated) for the open map is set to Default, the interpretation of the colors is as indicated in the table that appears in Figure 2. Note: If you have a color vision weakness, it is possible to change the colors displayed by HP OpenView. If you change them, make sure everyone who will use the software is aware of the changes.



Status Condition	Symbol Color	Connection Color
Unmanaged [(a)]	Off-white	Black
Testing [(a)]	Salmon	Salmon
Restricted [(a)]	Tan	Tan
Disabled [(a)]	Dark Brown	Dark Brown
Unknown [(o)]	Blue	Black
Normal [(o)]	Green	Green
Warning [(o)]	Cyan	Cyan
Minor/Marginal [(o)]	Yellow	Yellow
Major [(o)]	Orange	Orange
Critical [(o)]	Red	Red

[(a)] Administrative Status [(o)] Operational Status

Figure 2. HP OpenView Default Status Colors

Looking at maps for color alerts

To check your network for color alerts, you must first have the map for the network open. To open a map, use the following procedure:

Open a Network Map

1 With HP OpenView NNM running, follow menu path **Map→Maps→Open/List . . .**.

- The **Available Maps** dialog box is displayed.

2 Select the name of the map you want to open and click on "**Open Map**".

- A confirmation box is displayed.

3 Click on "**OK**".

- Any open map and its submap windows and dialogs close.
- The **Home Submap** (**Root**) of the selected map is displayed.

If you do not know the compound status scheme of the open map, follow the menu path **File→Describe/Modify Map** to obtain the **Map Description** dialog box and display/set the compound status scheme for default. Suppose there is a fault in an interface card in one of the workstations on your network. Use the following procedure to trace it using color alerts.

Looking at Maps for Color Alerts

1 Double click on the yellow **Internet** symbol.

- *Note*: The symbol will be yellow because the *critical* failure of the card in the workstation is propagated up to the level of the **Internet** symbol as a *minor* problem at that level.
- The **Internet submap** opens and displays the IP network(s). One IP network symbol is yellow. This indicates a marginal problem with the network.

2 Double click on the yellow **IP network** symbol.

- A **Network submap** opens and displays the segment(s) attached to the gateway(s). The segment symbol is yellow. This indicates a problem somewhere on the segment.

3 Double click on the yellow **segment** symbol.

- A **Segment submap** opens and displays the nodes attached to that segment. Of all the nodes in the segment, the workstation node is red. The problem is isolated to that workstation.

4 Double click on the red **workstation** symbol.

- A **Node submap** opens and displays its interface symbol. It is red.
- You have isolated the fault to a single card of a single node on your internet.

Looking at maps for new nodes

HP OpenView Windows includes an application called **IP Map** which, in default, is started automatically upon activation of HP OpenView Windows. IP Map creates network maps and submaps through several functions:

- automatically discovers all IP-addressable nodes on the network.
- creates an object for each discovered node.
- creates and displays symbols on the network map to represent created objects.
- creates a hierarchy of submaps to display the network in increasing detail.
  - internet submap.
  - network submaps.
  - segment submaps.
  - node submaps.

Each submap is assigned a layout algorithm that determines how its symbols are displayed. You can set automatic layout *on* or *off* to enable or disable enforcement of the layout algorithm, either for all submaps or for an individual submap. If autolayout is enabled, IP Map places new symbols directly on the submap. If autolayout is disabled, IP Map places new symbols in a **New Object Holding Area** in the lower part of the submap window. Symbols in the New Object Holding Area are shown without any connections. You can use HP OpenView to identify any new objects that are discovered and added to the open map. Suppose, for example, that a new workstation is added to the network and you wish to locate it and check its status. Use the following procedure to look for new nodes.

Looking at Maps for New Nodes

1 To check the default **Segment submap** for any new nodes that may have been discovered, open the default **Segment submap** from the segment symbol in the Network submap.

- View the submap for any new symbols.

2 To easily see new symbols in the submap, disable autolayout for the submap by following menu path **View→Automatic Layout→Off for this Submap**.

- When autolayout is disabled, a **New Object Holding Area** appears at the bottom of the submap.

- All newly added symbols are placed in the **New Object Holding Area**.

Creating special submaps for monitoring status

You can create submaps based on a logical organization rather than a physical one, to facilitate specialized monitoring. For example, suppose you want to have a submap just showing the Science Software Integration and Test (SSI&T) workstations at your site to have ready access to a display showing their status. Suppose further that you expect to use this submap frequently and therefore wish to create it within an existing hierarchy and be able to open it from a symbol in the Internet submap. Use the following procedure to create a special submap showing these workstations.

Creating Special Submaps for Monitoring Status

1 Decide where to locate your submap and whether it will have a parent or not.

- A submap without a parent object is independent of other existing submap hierarchies in the open map, and can be opened only from the **Available Submaps** dialog box. You can create child submaps of this submap, thereby creating a new submap hierarchy in the map.

- A submap that has a parent object can be opened from an explodable symbol of the parent object. If you want the new submap to exist within an existing submap hierarchy, you should create this submap from an explodable symbol.

2 To create a submap within an existing hierarchy, decide which symbol to use to open the new submap.

- If other symbols on the parent submap already open into child submaps or execute applications, you must create a new symbol to open the submap.

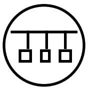
3 If you decide to create a new symbol (as in this case), add a symbol (for an existing object – in this case, a segment) or a new symbol and object to the submap of your choice (in this case, the Internet submap), by following menu path **Edit→Add Object . . .** .

- The **Add Object: Palette** window is displayed.

4 Click on the symbol representing the class of objects you want to add to the submap, using the scroll bar if necessary to scroll to the right for access to the desired symbol.

- For this training exercise, use the **Network Class**.
- The object symbols in the chosen class appear in the **Symbol Subclass** area of the **Add Object: Palette**.

5 Using the middle mouse button, drag the symbol representing the object to be added and drop it in the submap where it is to be added.

- You may add any of the symbols in the network class. For this training exercise, use the **bus** symbol ().
- The **Add Object** dialog box is displayed.

6 In the **Label Name** field of the **Add Object** dialog, type a label for the object (e.g., for this training exercise, type **SSI&T Workstations** and then click on the **OK** button.

- The entered label appears on the newly added blue symbol.

7 Open the new submap by double-clicking on the newly created symbol and then clicking on the **OK** button in the **Question** dialog that appears. Copy SSIS&T Workstation objects from other submaps into the newly created map, following menu path **Edit**→**Copy** and **Edit**→**Paste** operations.

- For more information about these operations, see the *HP OpenView Windows User's Guide*.

8 If desired, for each workstation copied, add its connection by following menu path **Edit**→**Add Connection . . .** .

- An **Add Connection** dialog is displayed, allowing you to select a type of connection (e.g., **Generic**), and then directing you to select a source and destination for the connection. You must then enter a selection name for the connection.
- When you click on **Close** for the **Add Connection** dialog, the newly added symbol changes color to indicate the status of its contained objects.

Checking for event notifications

Whenever a change occurs on the network, an **event** is generated. The occurrence of the event has two consequences:

- Through the internal processors of the **Network Node Manager**, the event is registered in a predefined category for display in an **Events Browser** window.

- The registration in the Events Browser window triggers a change for display in an **Event Categories** window (see Figure 3) to provide a notification that an event has occurred in the category of that Events Browser window. The display is a color change in a button on the Event Categories window corresponding to the event category. The color of the button indicates the highest severity event in the category. The default categories included in the Event Categories window are:

  – *Error Events*. This indicates inconsistent or unexpected behavior.

  – *Threshold Events*. This indicates that a threshold was exceeded.

  – *Status Events*. This indicates that an object or interface status changed to “up” or “down,” or an object or interface started or stopped responding to Internet control message protocol (ICMP) echo requests.

  – *Configuration Events*. This indicates a node’s configuration changed.

  – *Application Alert Events*. This indicates an HP OpenView Windows application generated an alarm or alert.

  – *All Events*. This indicates one or more of the previously listed events occurred. Selecting this button lists all events in the listed categories and others in one dialog box.

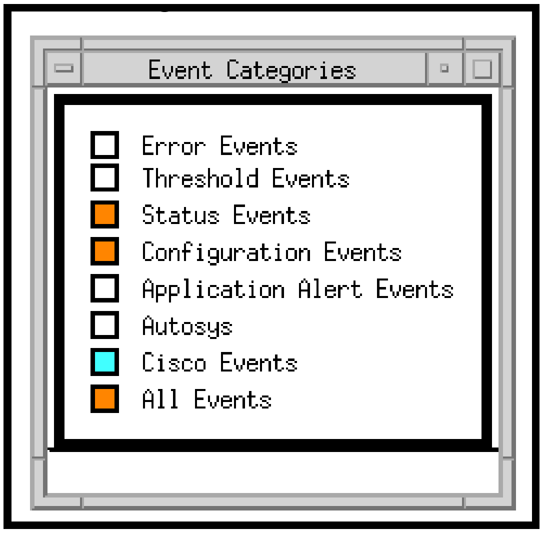


Figure 3. HP OpenView Event Categories Window

To check for event notifications, examine the Event Categories window to observe any color change in one or more of the buttons for the event categories. If there is a color change, you can click on the button to view its associated Events Browser window. For example, suppose you are monitoring the network when a critical threshold is exceeded somewhere on the network. Use the following procedure to check for event notifications.

Checking for Event Notifications

1 Observe that the **Threshold Events** button in the **Event Categories** window is red.

- This indicates that a critical threshold was exceeded somewhere on the network.

2 Click on the **Threshold Events** button in the **Event Categories** window. The **Threshold Events Browser** dialog box appears with a chronological listing of the threshold events that have occurred, with the most recent events at the bottom of the list.

- Each event listed includes the severity, time the event occurred, node on which the event occurred, and a brief event message.

3 To view the node that generated the event shown in this example, select the event from the list and click on **Action→Highlight Source on Map**.

- A map appears with the **busynode** node highlighted. At this point, select the highlighted node by clicking on it, and invoke appropriate operations from the menu bar to further diagnose and correct the situation which caused the threshold to be exceeded.

4 To delete the event, select the event and click on **Action→Delete→Selected Event**.

- This deletes only the selected event. (Note: multiple events may be selected and deleted.)
- For more information about event notification, click on the **help** button in the dialog box for the event being viewed or select **View SNMP Events** from the **Help: Index→Task**.

Accessing the EOSDIS Backbone Network (EBnet) Web Page

The EBnet is a Wide Area Network (WAN) that provides, in combination with other institutional and public networks, connectivity between geographically distributed EOSDIS facilities to support ECS mission operations and data production functions. Specifically, its functions include:

- provides connectivity between the ECS DAACs, the EOS Data and Operations System (EDOS) facilities, affiliated data centers, and other designated EOSDIS sites.
- serves as the interface between EDOS, the DAACs, and the NASA Science Internet (NSI).
- transporting spacecraft command, control, and science data nationwide on a continuous basis, 24 hours a day, 7 days a week.

- transports real-time mission-critical data related to the health and safety of on-orbit space systems and raw science telemetry as well as pre-launch testing and launch support.
- transports science data collected from spacecraft instruments and various levels of processed science data including expedited data sets, production data sets, and rate-buffered science data.
- provides wide-area communications through common carrier circuits for internal EOSDIS communications.
- interface to Exchange Local Area Networks (LANs) which provide communications between the WAN and site-specific LANs.

The NASA Communications (Nascom) organization at Goddard Space Flight Center (GSFC) maintains a home page for the EBnet (see Figure 4) on the World Wide Web at the following Universal Resource Location (URL):

- http://bernoulli.gsfc.nasa.gov/EBnet/.

This web site provides an overview of the EBnet as well as current data on its status and performance. Consequently, it can be a useful source of information when you are monitoring system performance. To access the EBnet Web Page, use the following procedure.

Accessing the EOSDIS Backbone Network (EBnet) Web Page

1 On workstation ***x*0MSH*##***, at the UNIX prompt in a terminal window, type **Netscape** at a UNIX command prompt and then press the **Return** key.

- NOTE: The ***x*** in the workstation name will be a letter designating your site: **g** = GSFC, **m** = SMC, **l** = LaRC, **e** = EDC, **n** = NSIDC, **o** = ORNL, **a** = ASF, **j** = JPL; the ***##*** will be an identifying two-digit number (e.g., **g0msh08** indicates a management services subsystem *hp* workstation at GSFC). If you access the workstation through a remote login (rlogin), you must enter **xhost +** prior to the rlogin, and enter **setenv DISPLAY <local_workstation IP address>:0.0** after the rlogin before entering the **Netscape** command.
- The starting page selected to appear on launch of the browser is displayed.

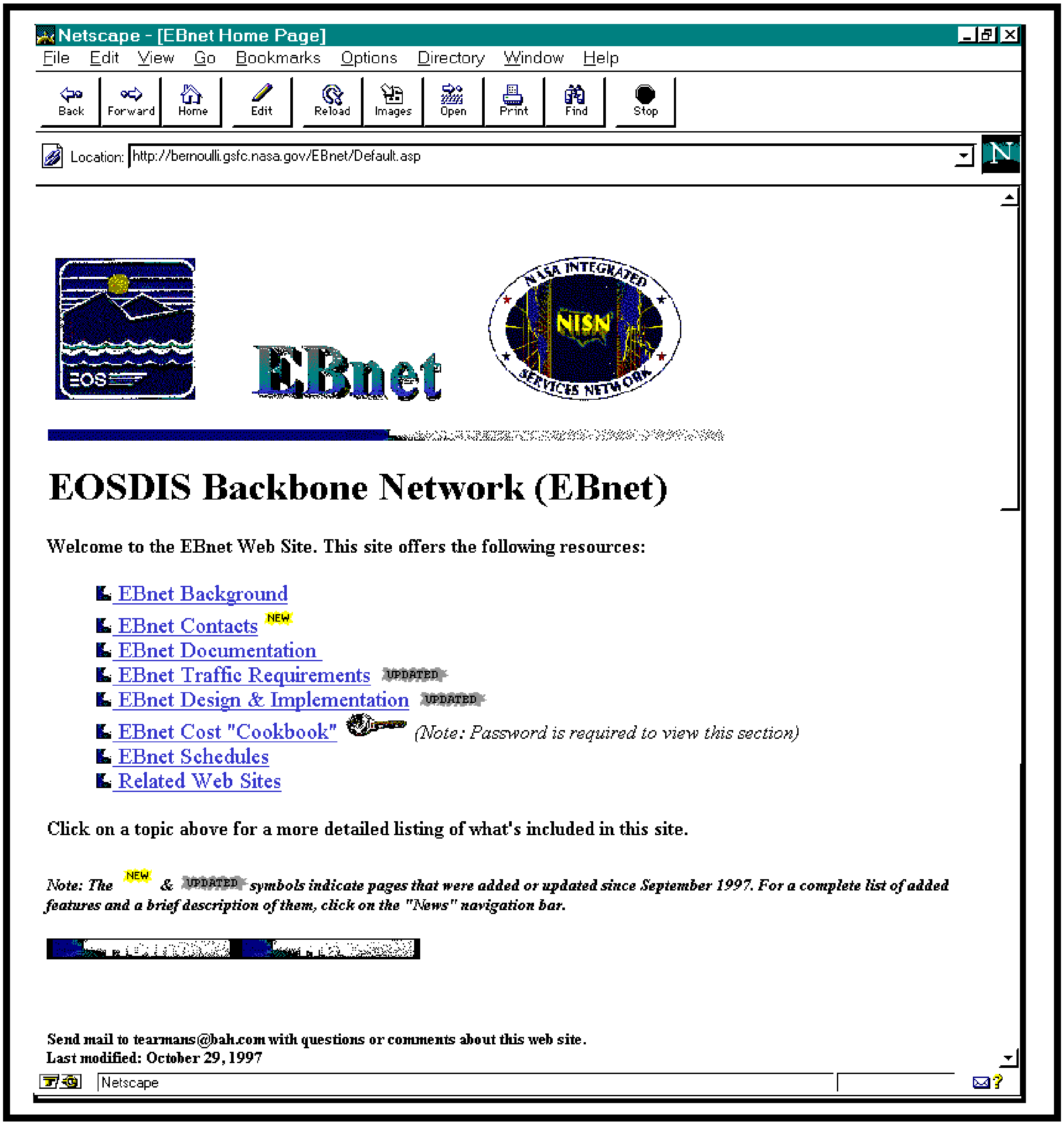
2 Click on the **Location** window of the starting page.

- The contents of the **Location** window are highlighted.

3 Enter **http://bernoulli.gsfc.nasa.gov/EBnet/** in the **Location** window.

4 Press the **Return/Enter** key on the keyboard.

- The EOSDIS Backbone Network (EBnet) home page is displayed.


Netscape - [EBnet Home Page]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://bernoulli.gsfc.nasa.gov/EBnet/Default.asp
EOS
EBnet
NASA INTEGRATED SERVICES NETWORK
NISN
Netscape

EOSDIS Backbone Network (EBnet)

Welcome to the EBnet Web Site. This site offers the following resources:

- EBnet Background
- EBnet Contacts NEW
- EBnet Documentation
- EBnet Traffic Requirements UPDATED
- EBnet Design & Implementation UPDATED
- EBnet Cost "Cookbook" *(Note: Password is required to view this section)*
- EBnet Schedules
- Related Web Sites

Click on a topic above for a more detailed listing of what's included in this site.

Note: The NEW & UPDATED symbols indicate pages that were added or updated since September 1997. For a complete list of added features and a brief description of them, click on the "News" navigation bar.

Send mail to tearmans@bah.com with questions or comments about this web site.
Last modified: October 29, 1997

Figure 4. EBnet Home Page

Problem Analysis/Troubleshooting

Although ECS is designed to be a robust computer network system, the complexity of its hardware and software components and interfaces provides a wealth of potential sources for system failures or other non-conformance problems. Fortunately, the tools available in ECS provide several avenues of assistance to help you detect and isolate problems in the system.

Analysis/Troubleshooting: System

Some of the Commercial Off-The Shelf (COTS) software products that are part of ECS provide alerts or warnings when there are system problems. For example,:

- HP OpenView.
  - color alerts to indicate problems.
- AutoSys/Xpert.
  - color/auditory alerts to indicate job status/failures.
- Tivoli.
  - "thermometer" icon showing high temperature to indicate failure.

Many of the COTS products as well as the software developed specifically for ECS generate error messages and event messages to indicate errors and status. The interpretation of these messages and suggested corrective actions can be found in 609-CD-003-001 *Operations Tools Manual*. Several products also generate logs to capture and provide more detailed information about indicated problems. For example,:

- HP OpenView.
  - event notifications/events browser; focus on all system events.
- Tivoli.
  - Tivoli Enterprise Console (TEC) system monitoring log; focus on software events.
- ClearCase®.
  - software installation error log files.

As of software Drop 4, ECS will also provide Management Data Access (MDA) services, including an event log browser, developed specifically to provide access to centralized information entered into the management data log file on each managed host from various sources. These log data include performance, security, fault, accountability, and other ECS application event information. The log browser can assist in troubleshooting through review of data on all significant system events in a single log. It allows an operator to browse events in the log file, created by a Management Services Subsystem (MSS) agent. The MSS agent is designed to capture and assign *levels of significance* or *event priorities* to ECS events. The levels are:

- *Low* – characterizes all types of events that are useful to record but do not have any adverse significance in the operational status of the system. These messages are recorded for the purposes of analysis by operations personnel, assert that something specific happened, or for the verification of a sequence of events. Typically, they are informational events (e.g., indication of current level of performance, status change, task completion).

- *Medium-Low* – messages of warnings or errors that are of low significance. They are recoverable problems that are useful to record for future analysis by operations personnel, asserting that something specific happened, or for the verification of a sequence of events (e.g., memory/stack overflow that is recoverable, recoverable data errors, recoverable arithmetic errors such as divide by zero).

- *Medium* – characterizes events that are potential indicators of future problems. They can also indicate abnormal system activity such as a transaction terminated abnormally, although the system remains fully operational. The event does not require immediate operational attention. It could be a warning or an error that operations personnel should note if it occurs with a particular frequency or if it is known to be a good indicator of a pending problem. Operations personnel typically will have to trace the cause of the abnormal event so that the system activity can be reinitiated, or to prevent the abnormal event from recurring. Such events may indicate a requirement for maintenance (e.g., performance threshold exceeded, uncorrectable communication errors and uncorrectable disk input/output error where retries were not successful, PGE terminated abnormally).

- *High* – characterizes error events which have an impact on operations. This level also characterizes abnormal events which are fatal to, or seriously degrade, the operation of a server/hardware equipment or to the interaction between servers and require immediate attention by the operator (e.g., Storage Manager terminated abnormally and Sybase SQL Server down, V0 Gateway down, FDDI switch inoperable, irrecoverable LAN failure).

The browser provides the option to open a log file of a specific host to sort and filter events to find detailed information on an event. It permits:

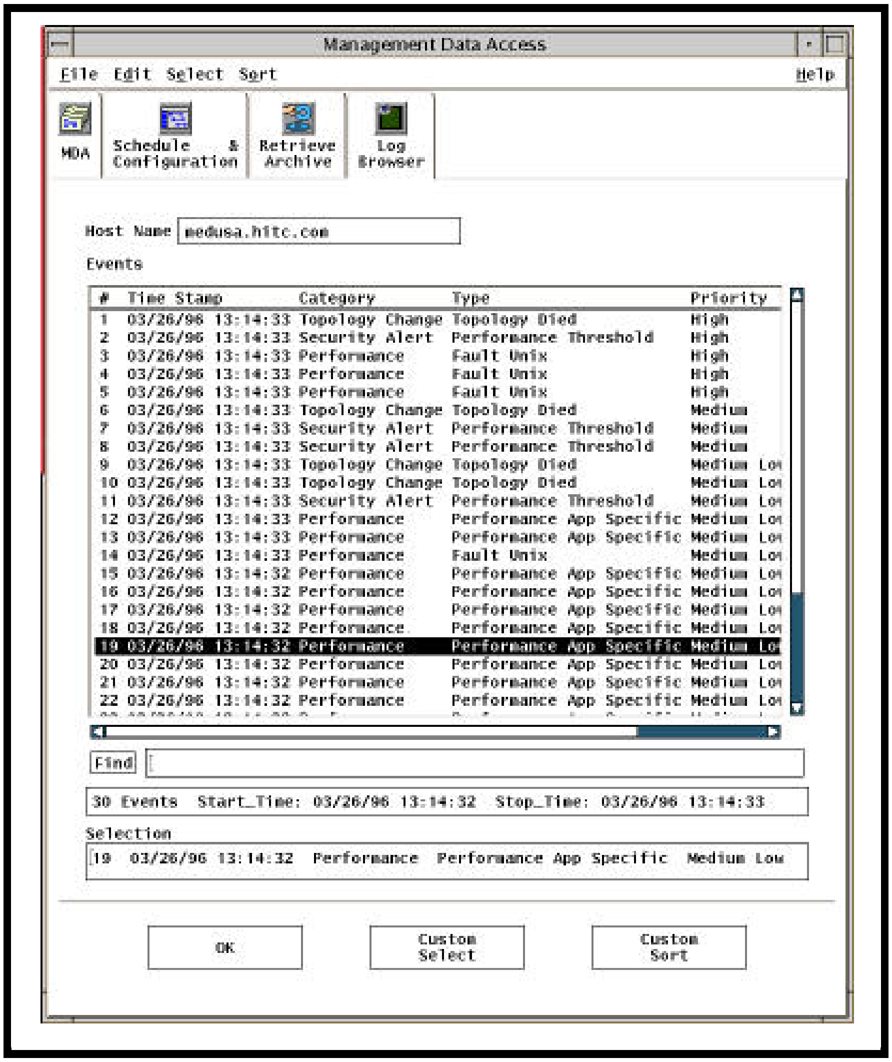
- selecting a log file -- choose from a list of log files on the MSS server to browse events from a selected host.

- filtering events -- creation of a customized filtering option to assist in finding a specific event.

- sorting events -- creation of a customized sort, including multi-level sorting and selection of sorting direction to assist in finding a specific event.

- viewing events -- listing of data in all fields to provide detailed information on an event.

Figure 5 shows the screen of the MDA application with the ECS Event Log Browser tab selected.



Host Name medusa.hitc.com

Events

```
#  Time Stamp        Category        Type                     Priority
1  03/26/96 13:14:33 Topology Change Topology Died            High
2  03/26/96 13:14:33 Security Alert  Performance Threshold    High
3  03/26/96 13:14:33 Performance     Fault Unix               High
4  03/26/96 13:14:33 Performance     Fault Unix               High
5  03/26/96 13:14:33 Performance     Fault Unix               High
6  03/26/96 13:14:33 Topology Change Topology Died            Medium
7  03/26/96 13:14:33 Security Alert  Performance Threshold    Medium
8  03/26/96 13:14:33 Security Alert  Performance Threshold    Medium
9  03/26/96 13:14:33 Topology Change Topology Died            Medium Low
10 03/26/96 13:14:33 Topology Change Topology Died            Medium Low
11 03/26/96 13:14:33 Security Alert  Performance Threshold    Medium Low
12 03/26/96 13:14:33 Performance     Performance App Specific Medium Low
13 03/26/96 13:14:33 Performance     Performance App Specific Medium Low
14 03/26/96 13:14:33 Performance     Fault Unix               Medium Low
15 03/26/96 13:14:32 Performance     Performance App Specific Medium Low
16 03/26/96 13:14:32 Performance     Performance App Specific Medium Low
17 03/26/96 13:14:32 Performance     Performance App Specific Medium Low
18 03/26/96 13:14:32 Performance     Performance App Specific Medium Low
19 03/26/96 13:14:32 Performance     Performance App Specific Medium Low
20 03/26/96 13:14:32 Performance     Performance App Specific Medium Low
21 03/26/96 13:14:32 Performance     Performance App Specific Medium Low
22 03/26/96 13:14:32 Performance     Performance App Specific Medium Low
```

```
30 Events  Start_Time: 03/26/96 13:14:32  Stop_Time: 03/26/96 13:14:33
```

Selection

```
19  03/26/96 13:14:32  Performance  Performance App Specific  Medium Low
```

Figure 5. Event Log Browser Window from MDA

Suppose you are analyzing a problem on one of the processors for Data Server; you have used HP OpenView to determine that the problem is with the host *x*0acg01 (where *x* is g, m, e, l, n, o, a, or j for GSFC, SMC, EDC, LaRC, NSIDC, ORNL, ASF, or JPL respectively) and you want to look at application-specific events on that host. Use the following procedure to call up the MDA Event Log Browser file for that host, sort the listed events by subsystem and type of event, and select events for the Data Server Subsystem (DSS).

Review Event Log Browser

1 Click on the **MDA** icon from the ECS Desktop.

- The **MDA** main screen is displayed.

2 Click on the **Log Browser** tab.

- The **Event Log Browser** screen is displayed.

3 Follow menu path **File→Open**.

- The **File Selection** dialog box is displayed.

4 Highlight the file name for the desired host (in this case, *x*0acg01) and Click on the **OK** button.

- The list of events is displayed in the **Events** window.

5 Click on the **Custom Sort** button.

- The **Custom Sort** dialog box is displayed.

6 Click on the **Sort By:** buttons for **Type** and **Subsys** and then **Click** on the **OK** button.

- The listed events are sorted by type and subsystem.

7 Click on the **Custom Select** button.

- The **Custom Select** dialog box is displayed.

8 Click on the **Subsystem** pop-down pick-list and select the desired subsystem (in this case, **DSS**).

- The **Event** window displays only events for the selected criteria.

As is ever the case with a complex system, the effectiveness of troubleshooting depends on knowledge of the system and its documentation, applied systematically to diagnose problems. Your knowledge and skill may be called upon only after a user or an operator has already attempted some problem solving (e.g., based upon error messages displayed directly to the screen) and then submitted a trouble ticket. The effectiveness of your troubleshooting is maximized by:

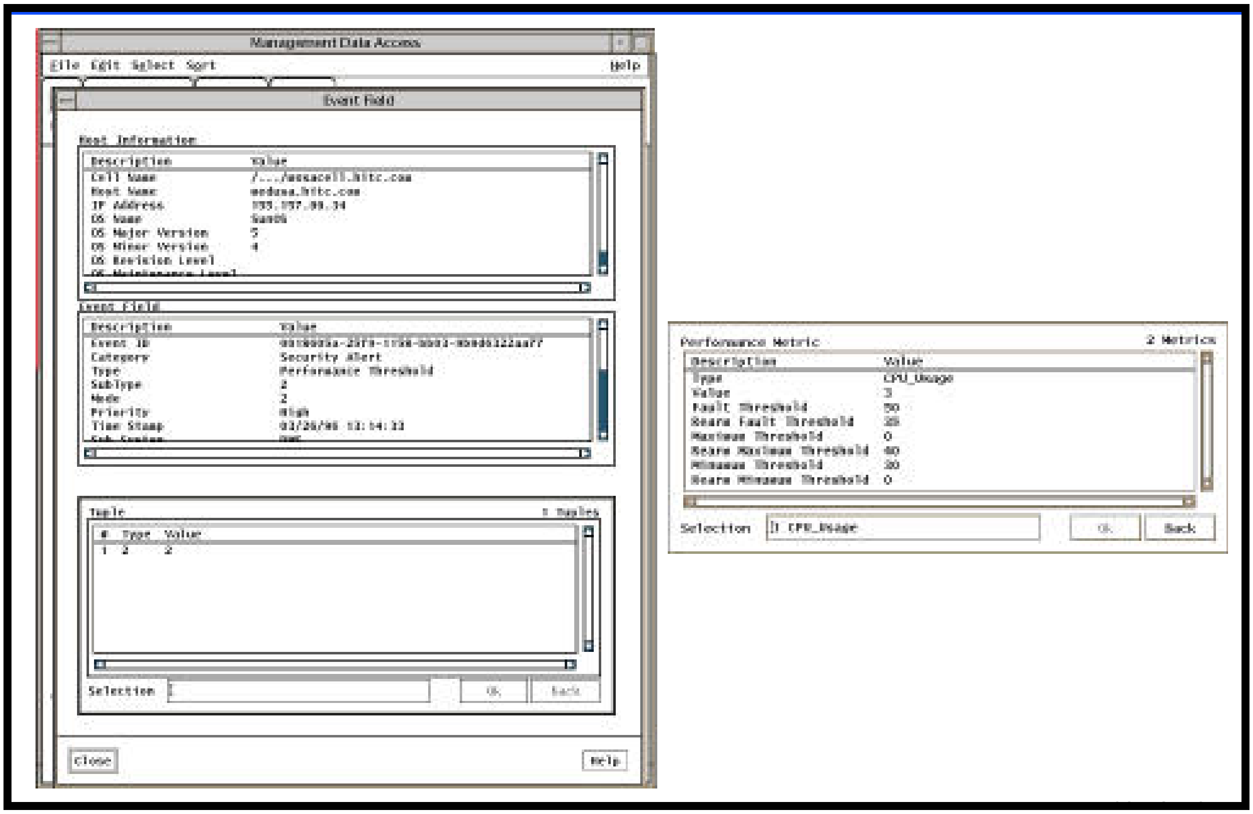
- thorough documentation of the problem.
  - date/time of problem occurrence.
  - hardware/software.
  - initiating conditions.
  - symptoms.

- verification.
  - identify/review relevant publications (e.g., COTS product manuals, ECS tools and procedures manuals).
  - replicate problem.
- identification.
  - review product/subsystem logs.
  - review HP OpenView Event Browser.
- analysis.
  - detailed event review (e.g., HP OpenView Event Browser Event Fields).
  - determination of cause/action.

For analysis, the Event Log Browser provides a detailed event field list showing specific information or messages associated with an event. Information in the event fields is of two types:

- performance metrics – data reflecting measured values of system or application performance associated with an event (e.g., time, number of elements, rates).
- tuples – data reflecting unique strings of information associated with and descriptive of an event (e.g., names, identifier numbers, data types).

Figure 6 shows examples of the detailed event fields from the Event Log Browser. System operators may set thresholds associated with these information metrics/tuples, which provides a way to obtain additional detail for troubleshooting.



Host Information

Description	Value
Cell Name	/.../ecsacell.hitc.com
Host Name	medusa.hitc.com
IP Address	155.157.99.34
OS Name	SunOS
OS Major Version	5
OS Minor Version	4
OS Revision Level	
OS Maintenance Level	

Event Field

Description	Value
Event ID	[illegible]
Category	Security Alert
Type	Performance Threshold
SubType	2
Mode	2
Priority	High
Time Stamp	03/26/96 13:14:33
Sub System	DMS

Tuple 1 Tuples

#	Type	Value
1	2	2

Selection 1

Performance Metric 2 Metrics

Description	Value
Type	CPU_Usage
Value	3
Fault Threshold	50
Rearm Fault Threshold	25
Maximum Threshold	0
Rearm Maximum Threshold	40
Minimum Threshold	20
Rearm Minimum Threshold	0

Selection 1 CPU_Usage

Figure 6. Log Browser Event Field Screens

An Event Field Screen may be accessed by double clicking on one of the events listed in the Event window of the Event Log Browser.

Analysis/Troubleshooting: COTS Hardware

The ECS hardware is composed almost entirely of commercial, off-the-shelf (COTS) products, for which there are vendor maintenance warranties and/or COTS hardware support contracts. When a system problem is discovered, there is an initial troubleshooting/diagnostics procedure to be followed which is generic – i.e., not limited to hardware problems. However, when a hardware problem is indicated, the procedure refers the problem to the Maintenance Coordinator for hardware corrective maintenance. System troubleshooting tools and principles apply:

- HP OpenView for quick assessment of status.
- MDA Event Log Browser for sequence of events.
- Initial troubleshooting.
  - – Review error message against hardware operator manual; prepare trouble ticket.
  - – Verify connections (power, network, interface cables).
  - – Run internal systems and/or network diagnostics.

  - Review system logs for evidence of previous problems.
  - Attempt system reboot.
  - If problem is hardware (e.g., software has been working and reboot is unsuccessful), report it to the Maintenance Coordinator – i.e., forward the trouble ticket.

A problem that is not resolved through initial troubleshooting will often require troubleshooting teamwork by the Maintenance Coordinator, the System Administrator, and perhaps a Network Analyst. These troubleshooters may perform additional steps to resolve the problem:

- specific troubleshooting procedures described in COTS hardware manuals.
- non-replacement intervention (e.g., adjustment).
- replace hardware with maintenance spare.
  - locally purchased (non-stocked) item.
  - installed (hot-swappable, excess capacity) spares (e.g., RAID storage, power supplies, network cards, tape drives).

If the hardware problem is not resolved by the actions of the local staff, it may be necessary to request assistance through the Maintenance Coordinator from a maintenance contractor for on-site hardware support. Suppose, for example, that you are a Maintenance Coordinator and HP OpenView has indicated a problem with one of the Sun workstations, that initial troubleshooting finds the workstation to be inoperable, that a trouble ticket has been forwarded to you, and that you and System Administrator are not able to resolve the problem through additional troubleshooting. That workstation is hard down. The correct approach is:

- Organize the data on the problem, find data on the appropriate support provider, and update the trouble ticket with this information.
- Call the support provider’s technical support center to obtain on-site assistance.
  - Provide them with the background data.
  - Obtain a case reference number from them.
  - Update the trouble ticket to reflect the time and date of the call and the case number.
  - Notify the originator of the problem that the contractor is on the way.
- Arrange for site access for the maintenance technician.
  - Record arrival time.
  - Escort technician to hardware.

    - Assist in problem resolution (e.g., arrange equipment shutdown, demonstrate problem).

    - Obtain any needed technical references that are available at the site.

- Update trouble ticket with actions taken to correct the problem and delay time experienced for the repair, including start/stop times and reasons for each delay

- For any replaced part, update the trouble ticket with additional supporting data.

    - Part number of the new item.

    - Serial numbers of the old and new items.

    - Equipment Identification Number (EIN) assigned to the new item (if applicable).

    - Model number of replacement Line Replaceable Unit (LRU). [Note: If the model number of the replacement LRU is different from the part removed, a configuration change request (CCR) is required for configuration management.]

    - Name of the item replaced.

In preparation to request on-site hardware support from the maintenance contractor to repair the down Sun workstation, use the following procedure to obtain the background information needed.

Obtaining On-Site Hardware Support: Background Information

1 Collect information needed to obtain contract maintenance support.

- Obtain **make**, **model**, **serial number**, and **location** of the failed system from the hardware database.

- Obtain description of problem and symptoms from **trouble ticket**.

- Identify the **criticality** of the COTS hardware experiencing the problem.

2 Determine maintenance provider data.

- Obtain **name**, and **telephone number** of the maintenance provider.

- Obtain **access code** needed to obtain support.

- Obtain **telephone number** of the support provider’s technical support center.

- Obtain **name** of site authorized contact person.

3 Record data on maintenance needed and maintenance provider into the trouble ticket.

In unusual cases, it may be necessary to resort to non-standard hardware support procedures. In the event that the maintenance contractor's assigned technician is not providing timely successful repair, or if the maintenance action is otherwise unsatisfactory, it may be necessary to escalate the problem to bring it to the attention of the support contractor's management. The escalation is achieved by calling the maintenance contractor's technical support center and providing them with the case reference number. Another non-standard support approach, which may be costly and is to be used only as a last resort for mission-critical repairs, is Time and Material (T&M) support. For T&M support, the local Maintenance Coordinator must obtain authorization from the ILS Maintenance Coordinator or, if that person is unavailable, from the Sustaining Engineering Organization (SEO).

Performing Preventive Maintenance

The only hardware that may require scheduled preventive maintenance is the E-Systems Modular Automated Storage Systems (EMASS) robot.

- Scheduled by the local Maintenance Coordinator.
- Coordinated with maintenance organization and using organization.
  - Scheduled to be performed by maintenance organization and to coincide with any corrective maintenance if possible.
  - Scheduled to minimize operational impact.
- Documented using a trouble ticket.

Analysis/Troubleshooting: COTS Software

The maintenance of COTS software items in ECS requires the management of software maintenance contracts with software vendors. This element includes:

- maintaining software use licenses.
- obtaining telephone assistance in resolving COTS software problems.
- obtaining software patches.
- obtaining software upgrades.

COTS software vendor support is contracted by the ECS procurement office at the ECS Development Facility (EDF).

- First year is under warranty support.
- Subsequent support is acquired through contract extension/modification as needed.
- COTS software support contracts data are maintained in a database used by the ECS Integrated Logistic Support (ILS) office to monitor and track contract expiration dates and terms.

- Local Maintenance Coordinators (LMC) can request changes to COTS software support contracts by contacting the ILS Logistics Engineer.
  - Contact by e-mail can be made by using **ilsmaint@ecs.hitc.com** as the address.
  - Contact by telephone can be made by using the number 1-800-ECS-DATA (1-800-327-3282), selecting Option #1, and then requesting the ILS Logistics Engineer.

COTS Software Licenses

Licenses to use COTS software vary by the type of software and the software vendors' policies. License types include:

- per seat.
- per site.
- specific number of concurrent users.
- unlimited users.
- lifetime use without regard to number of users or location.

COTS software licenses are maintained in a property database. The ECS Property Administrator:

- maintains the master copy of COTS software license agreements.
- maintains the COTS software license database.
- distributes COTS software for installation at the DAACs.

The ECS Program reflects several different license restrictions based on the license types negotiated for the different COTS software products used. In general, the license restrictions are imposed through a software program that runs on a license server at the DAAC. It tracks the instances of a program in use, and when the limit is reached, it precludes access by additional operators until use falls below the limit. Table 1 lists four of the major COTS packages and identifies the license restrictions that apply to each.

Table 1. Major COTS Software License Restrictions

Software	Restriction
HP Open View	One site license, unlimited users
AutoSys	Only 1 instance at a time may be active
ClearCase®	5 users concurrently
DDTS	Virtually unlimited (10,000 users)

Installing COTS Software

The approval of appropriate CCBs is required prior to the loading of COTS software upgrades or other packages on any ECS platform. The approval process requires systematic Configuration Management (CM) procedures and documentation to ensure appropriate control of the ECS baseline and of changes to the baseline. Once the approval is received, the site Local Maintenance Coordinator notifies those personnel who will accomplish the installation (e.g., Release Installation Team, System Administrator, Network Administrator, Software Maintenance Engineer).

For ECS, there is one major tool used to facilitate CM control of software installation:

- **ClearCase**® – Provides a mountable file system which is used to store version-controlled data, such as source files, binary files, object libraries and spreadsheets.

The ClearCase® tool is used primarily for the ECS Science Software Integration and Test (SSI&T) function, but it is also applied to control changes in custom software and customized portions of some COTS software packages (e.g., configuration files).

At the DAAC, the COTS software installation actions are executed by the DAAC Software Maintenance Engineer and the System Administrator. Installation proceeds systematically. The installation is generally straightforward:

- the COTS software is installed with any ECS customization (e.g., configuration files).

- the Version Description Document (VDD) gets final updates for system and center-specific material identified by ESDIS or the operational centers, and the final VDD is available.

Safeguarding COTS Software Media

Any residual COTS software media and commercial documentation should be protected by appropriate means. For example, it may be desirable to store them in locked cabinets provided for the purpose at the DAAC. Should there be a need for access to these materials (e.g., a requirement to reload a COTS software product), keys for these cabinets can be made available from the Operations Coordinator during operating hours.

Obtaining COTS Software Support

Support of COTS software involves both site capability and contracted support. Site support is provided by the System Administrator and the Software Maintenance Engineer. When site support personnel confirm that a problem is attributable to the COTS software, the COTS Software vendor's technical support center/help desk is contacted by authorized personnel at the site. When a system problem is discovered, there is an initial troubleshooting/diagnostics procedure to be followed which is generic – i.e., not limited to software problems. However, when a software problem is indicated, the procedure refers the problem to the Maintenance Coordinator for software corrective maintenance. System troubleshooting tools and principles apply:

- Software package event browser (e.g., MDA Event Log Browser) for sequence of events.
- Initial troubleshooting.
  - Review error message against software operator manual; prepare trouble ticket.
  - Review system logs for evidence of previous problems.
  - Attempt software reload.
  - If problem is software (e.g., hardware has been working and reload does not correct the problem), report it to the Maintenance Coordinator – i.e., forward the trouble ticket.

A problem that is not resolved through initial troubleshooting will often require troubleshooting teamwork by the Maintenance Coordinator, the System Administrator, and perhaps a Network Analyst. These troubleshooters may perform additional steps to resolve the problem:

- specific troubleshooting procedures described in COTS software manuals.
- review of the software vendor's web site's solutions database to learn of any solutions for similar problems.
- exercise any embedded or down-loadable software diagnostic routine that will determine the status of the COTS software on the equipment.
- exercise of any locally devised troubleshooting/diagnostic procedures.
- non-replacement intervention (e.g., adjustment of thresholds or other tunable parameters).

If the software problem is not resolved by the actions of the local staff, it may be necessary to request assistance through the Maintenance Coordinator from a maintenance contractor for on-site software support. Suppose, for example, that you are a Maintenance Coordinator and the site Software Maintenance Engineer has determined there is a problem with one of the COTS software packages used for Configuration Management, that initial troubleshooting finds the problem unable to be corrected locally, that a trouble ticket has been forwarded to you, and that you and System Administrator are not able to resolve the problem through additional troubleshooting. The correct approach is:

- Organize the data on the problem, find data on the appropriate support provider, and update the trouble ticket with this information.
  - Locate information such as software vendor technical support center/help desk telephone numbers, names of personnel authorized (by site and software) to contact the vendor, and the authorization/access codes available to the site's Local Maintenance Coordinator from the ECS ILS office.
- Contact the support provider's technical support center/help desk to obtain on-site assistance.
  - Provide them with the background data.
  - Obtain a case reference number from them.
  - Update the trouble ticket to reflect the time and date of the call and the case number.
  - Notify the originator of the problem that the contractor has been alerted to the problem.
- Maintain coordination with the vendor for the solution and ensure compliance with Configuration Management requirements.
  - Software vendor's technical support center/help desk verifies contract support authorization and assists in pinpointing the COTS software problem to provide a recommended solution.
  - Solution may include a patch, a work-around, or a fix in a future release of the software.
  - Assist in problem resolution (If a patch exists to correct the problem, the patch will be identified and provided by the software vendor over the Internet or mailed to the requester. If a patch is required but not available, the requester and the vendor together determine the seriousness of the problem. If the problem is critical, a temporary patch or work-around may be provided, with permanent solution to be implemented in a future update or release.).
  - The DAAC and Project Configuration Control Boards (CCBs) must authorize the patch to be installed as a permanent solution. This decision may be made after the fact, in accordance with emergency procedures required to continue to operate.

- Update trouble ticket with actions taken to correct the problem and delay time experienced for the solution, including reasons for each delay.

In preparation to request software support from the software vendor to resolve the problem, use the following procedure to obtain the background information needed.

Obtaining On-Site Software Support: Background Information

1 Collect information needed to obtain contract maintenance support.

- Obtain **version**, **release**, **serial number**, and **location** of the failed software from the software database.
- Obtain description of problem and symptoms from **trouble ticket**.
- Identify the **criticality** of the COTS software experiencing the problem.

2 Locate information on the software support vendor.

- Obtain **name**, and **telephone number** of the software support vendor.
- Obtain **access code** needed to obtain support.
- Obtain **telephone number** of the software support vendor's technical support center.
- Obtain **name** of site authorized contact person.

3 Record data on maintenance needed and maintenance provider into the trouble ticket.

In unusual cases, it may be necessary to resort to non-standard software support procedures. In the event that the software support vendor's technical support center/help desk is not providing timely successful solutions, or if the maintenance action is otherwise unsatisfactory, it may be necessary to escalate the problem to the ECS Sustaining Engineering Organization (SEO). The SEO is staffed with senior systems engineers knowledgeable on COTS software and can assist with diagnosing the problem. The site Local Maintenance Coordinator may go directly to the software vendor or to the ILS Logistics Engineer to obtain an escalation of software vendor support, resulting in increased vendor management review of the problem resolution, the assignment of additional resources to resolve the problem, and/or a more highly qualified technician assigned to resolve the software problem.

Troubleshooting of Custom Software

During operations, master copies of the custom software code are maintained at the ECS Development Facility (EDF). However, there may be a need for the M&O organization to modify the configuration as established at each center.

- Software Change Manager, ClearCase®, provides the vehicle to store and maintain the local library.
- Governing policies and minimum developed software component level that may be removed from (checked out for maintenance) or reintroduced to the master library are defined by the developers' determination of code modules.
- Configuration Management (CM) requirements apply (e.g., for configuration identification, configuration change control, and configuration status accounting).

Maintenance changes to the ECS baseline may come from any of several sources, such as:

- ESDIS CCB-directed changes.
- Site-level CCB-directed changes to configuration items, subject to ESDIS delegation of responsibility for site-level control.
- Developer modifications or upgrades.
- User- or operator-initiated trouble tickets.

Implementation of Modifications

A controlled build procedure provides structure for the implementation of changes.

- Each ECS organization selects a responsible engineer (RE) for each build.
- The SEO RE establishes the set of CCRs to be included in the system build.
- Site/center REs determine applicability of any site-unique extensions for the build.
- System and center REs establish schedules for implementation, integration, and test.
- The SEO RE maintains the integrated system- and center-specific CCR list and schedule.
- The SEO RE maintains the VDD, updating it with authorized changes. Center REs provide appendices as needed to describe any center-unique additions/modifications to the build.
- The RE (or designated team) for a CCR uses the configuration-controlled library to obtain the correct version of the source code/files. The RE/team implements the change, performs programmer testing, and updates the documentation (design, interface, and procedures documents).

Obtaining Custom Software Support

The maintenance of science software and data items provided by the Science Computing Facilities (SCFs) is not the responsibility of the ECS on-site maintenance engineers. Problem resolutions and changes to this software will be handled under the auspices of local DAAC CM activities and the ESDIS CCB in the same manner as new releases to baselined science software.

Problems with ECS custom software are one type of impetus for generating trouble tickets (TTs):

- Anomalies.
- Apparent incorrect execution by an ECS software configuration item.
- Inefficiencies.
- Sub-optimal use of system resources.
- TTs may be submitted by users, operators, customers, analysts, maintenance personnel, and management staff.
- TTs capture supporting information and data related to the problem.

Troubleshooting is conducted on an ad hoc basis. Just as with COTS software problems, however, it is conducted systematically.

- Site-level activity is initiated by the Operations Supervisor assigning a trouble ticket to the Problem Investigator.
- Problem Investigator uses list of Responsible Engineers if needed to obtain support from SEO Maintenance Programmers, Responsible Engineers, and ECS Developers at the ECS Development Facility (EDF).
- EDF has the same software and computer equipment variants available at the sites, and may be able to duplicate anomalies experienced in an on-site system to derive effective resolutions or work-arounds as required until a permanent solution can be implemented.
- At a TT telecon, the Failure Review Board assigns a priority to the TT and assigns the TT to an organization for work-off. The organization assigns a Responsible Engineer to work off the TT. Using the data captured in the TT, the Responsible Engineer conducts a technical investigation to attempt to isolate the source of the reported problem.
- If the problem is caused by a non-ECS element (e.g., an interface problem with an external system, poor resource usage by a science algorithm, poor performance by a non-ECS service), the TT and supporting data are provided to the maintainer of that element. An ECS CCR may also be proposed to protect ECS from potential threats of future problems identical or similar to that documented in the TT.

Trouble Ticket (TT)

We have seen that a system problem is typically documented using the Remedy COTS software product to prepare and update a problem report or trouble ticket (TT). Because there is a separate lesson that covers writing a trouble ticket, documenting changes, preparing and processing a trouble ticket through the Failure Review Board, and making emergency fixes, these topics are not addressed in detail here. By now you are familiar with the requirements for using trouble tickets in ECS problem management. You know that it is important to remember that high priority issues must be reviewed by the Failure Review Board (FRB), and that troubleshooting and repair activities that involve changes to the system configuration require a configuration change request (CCR).

Using Problem Report Software

Although you are familiar with using Remedy to create and view trouble tickets, there are other functions associated with the maintenance and operation of the trouble ticket service that you may be required to manage as a System Administrator or other manager. Specifically, the following tasks associated with Remedy may be required of the indicated administrator or others:

- adding users to Remedy — Database Administrator
- controlling and changing privileges in Remedy — Configuration Management Administrator
- modifying Remedy's configuration — Configuration Management Administrator.
- generating Trouble Ticket reports — System Administrator, others.

Let's look at each of these functions.

Adding Users to Remedy

The Database Administrator uses the Remedy RelB-User schema to grant access to the Remedy tool. Users who change jobs can be deleted. The Remedy *Administrator's Guide for OSF/Motif*, Chapter 3, "Setting Up Users and Groups," provides detailed instructions and information about license limitations. There are no license restrictions on the number of users who can be granted permission to create and query trouble tickets.

Figure 7 shows the screen layout for the Remedy RelB-User schema that is used for adding users. This screen is accessible to administrators with Administrator Group privileges by entering a Unix command beginning with the directory where Remedy is installed and invoking the user tool (e.g., **<*ar_install_dir*>/bin/aruser &**). This results in display of the user tool, from which you launch the RelB-User schema.

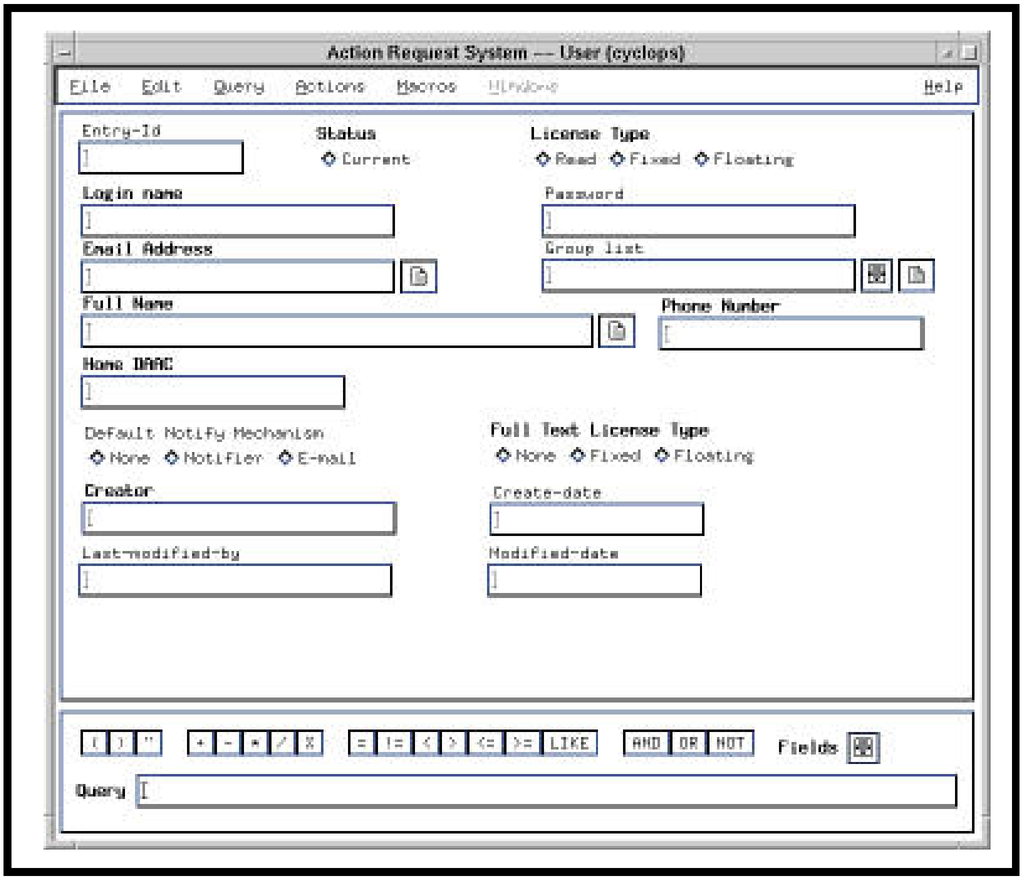


Figure 7. Remedy RelB-User Schema

Suppose, for example, that you wish to add Terry Bulticketer from the GSFC DAAC as a user with submit and query permissions. His e-mail address is tbultick@ecsgsfc1.gsfc.nasa.gov, and his phone number is 301-614-4132. The data to be entered to add a user include:

- Status – is the user current or not?
- License Type – what type of license does the user have? The default, **Read**, includes submit and query permission.
- Login Name – the identifying name the user will enter to use the Remedy tool.
- Password – the identifying password the user will enter to use the Remedy tool.
- Email Address – the e-mail address of the user.
- Group List – specifies a user's access control groups; must be left empty to grant only basic submit and query privileges.
- Full Name – the user's full name.
- Phone Number – the user's telephone number.

- Home DAAC – the user’s home DAAC.
- Default Notify Mechanism – the way in which the user will be notified of actions; if left blank, the method can be specified at the time an action is taken.
- Full Text License – the type of full text search license the user is to have; the default is **None**, which is what most users will be assigned (the number of full-text search licenses is limited).
- Creator – the person who created the account.

The system generates the content of the other fields. Use the following procedure.

Adding a User to Remedy

1 Follow menu path **File**→**Open Schema**.

- The **Open Schema** dialog box is displayed.

2 Double click on **User** from the list in the Open Schema dialog box, or click on **User** to highlight it and then click on the **Apply** button to load the schema.

3 Follow menu path **File**→**Open Submit**.

- A **Submit** window is displayed.

4 Click on the toggle button in front of **Current** to indicate the user’s status.

5 Click on the toggle button in front of the desired license type (in this case, **Read**).

6 Enter the login name (in this case, **tbultick**) to be used to access Remedy into the **Login Name** field..

7 Enter the identifying password into the **Password** field.

- You may wish to use the login name (in this case, **tbultick**), which the user can change upon first login.

8 Enter the user's e-mail address (in this case, **tbultick@ecsgsfc1.gsfc.nasa.gov**) in the **Email Address** field.

9 Enter the user's full name (**Terry Bulticketer**) in the **Full Name** field.

10 Enter the user's telephone number (**301-614-4132**) in the **Phone Number** field.

11 Enter the user's home DAAC (**GSFC**) in the **Home DAAC** field.

12 If you wish to select a default notification mechanism (e.g., e-mail), click on the toggle button in front of the desired selection (in this case, **E-mail**).

13 For **Full Text License Type**, ensure that the default, **None**, is selected; if necessary click on the toggle button in front of **None**.

14 Enter your name in the **Creator** field.

15 Click on the **Apply** button.

Changing Privileges in Remedy

Changing privileges in Remedy, or controlling privileges of those who have access to Remedy, is done by the Configuration Management Administrator. There are 18 Remedy privilege groups for ECS, and a change to the privileges of any group requires an approved Configuration Change Request (CCR). Access privileges provide permission to view a field, or to change it. The groups and their access privileges are defined in Document 611-CD-004-001 *Mission Operation Procedures for the ECS Project*, Section 8.2.6.

The Remedy *Administrator's Guide for OSF/Motif*, Chapter 3, "Setting Up Users and Groups," provides detailed information about access control and privileges. The administrator defines groups of users by using the User Tool to change the Group schema. A user's privileges may be changed in two ways:

- changing the group to which the user is assigned.
- changing the access privileges of the group.

We have seen that group assignment is accomplished using the RelB-User schema. Changes to the access privileges of a group is accomplished through use of the Admin tool, accessible by entering a Unix command beginning with the directory where Remedy is installed and invoking the tool with an option (e.g., **<*ar_install_dir*>/bin/aradmin -s &**). Use of the option **-s** in this way results in display of the Admin tool with the Schemas category displayed in the list. You can then define group access for schemas (Remedy databases) using the following procedure.

Defining Group Access for Schemas

1 Follow the **Categories**→**Schemas** menu path of the Admin Tool main window

- The **Group Access** item under the **Edit** menu is enabled.

2 Follow menu path **Edit**→**Group Access**.

- The **Group Access** window is displayed

3 Click on the **Group** list icon.

- The **Groups** dialog box is displayed.

4 Select a group from the dialog box, then click on the **Apply** button (or double-click on the entry.)

- The Group Access window then lists all current permission settings for that group for all items in the current category.

5 For each item, set the schema permissions for the specified group. Selecting **Yes** gives the group permissions to access the schema.

6 Click on the **Apply** button.

- The option settings are saved.

The Group Access – Schema Fields window allows you to determine **View** or **Change** access to field data. The following procedure is applicable.

Defining Group Access for Schema Fields

---

1 Follow the **Categories**→**Schemas** menu path of the Admin Tool main window

- The **Schema List** is displayed in the **Admin Tool**.

2 From the **Schema List** in the **Admin Tool**, open a schema by double clicking on it.

- The **Modify Schema** window is displayed.

3 Follow menu path **Attributes**→**Field Group Access**.

- The **Group Access – Schema Fields** window is displayed.

4 Click on the **Group** list icon.

- The **Groups** dialog box is displayed.

5 Select a group from the dialog box, then click on the **Apply** button (or double-click on the entry.)

- The **Group Access – Schema Fields** window displays buttons that differ according to the group chosen.

- Groups with a group type of **View** only allow you to select View permissions for schema fields.

- Groups with a group type of **Change** allow you to select View and Change permissions.

6 Set the permissions for each field.

- Selecting **View** allows users to view the field data in the schema. Selecting **Change** allows users to view and change the field data in the schema.

7 Click on the **Apply** button.

- The permission settings are saved.

8 Click on the **Apply** button in the Modify Schema window.

- The changes are now applied to the schema.

Changing Remedy Configuration

The RelB-Trouble Ticket schema, or Trouble Ticket screen, contains several fields that provide picklists, or pull-down lists of valid entries from which a user can select in filling out a trouble ticket. During ECS deployment, it may be necessary or desirable to change the items in some of these picklists. The fields that provide picklists that may be modified are:

- Closing Codes.
- Software Resources.
- Hardware Resources.
- Key Words.
- Problem Type.
- Forward-to.

The pull-down pick-lists in the RelB-Trouble Ticket schema can be customized by those given appropriate access. This is accomplished through the Admin Tool by modifying the **RelB-Menu-Closing Codes**, **RelB-Menu-Hardware Resources**, **RelB-Menu-Software Resources**, **RelB-Menu-Key Words**, **RelB-Menu-Problem Type**, and **RelB-TT-Sites** (for selection of the site to which a trouble ticket is forwarded) schemas. Procedure 8.2.7 in Document 611-CD-004-001 *Mission Operation Procedures for the ECS Project* refers to appropriate sections in the Remedy User’s Guide and the Remedy Administrator’s Guide. An approved Configuration Change Request (CCR) is required before implementing any of these changes. Modifying Remedy’s Configuration uses the following procedure.

Modifying Remedy's Configuration

1 Follow the **Categories→Menus** menu path of the Admin Tool main window

- The **Menu List** is displayed in the **Admin Tool**.

2 From the **Menu List** in the **Admin Tool**, open a menu by double-clicking on it.

- Select from the list one of the following: **RelB-Menu-Closing Codes**, **RelB-Menu-Hardware Resources**, **RelB-Menu-Software Resources**, **RelB-Menu-Key Words**, **RelB-Menu-Problem Type**, and **RelB-TT-Sites**.

- The **Modify Menu** window is displayed.

3 Select the level for which you want to add or modify menu choices by selecting the radio button next to the level's label.

- To add or modify menu choices at the highest level, select Level 0. Select each successive menu level to modify the choices at that level.

- Menu choices added at levels below the top level (level 0) will be sub-items of the selected item at the next highest menu level.

4 Enter a label (the text that will show up in the menu).

- Enter a maximum of 30 characters.

5 If the text that you want to appear when the user selects this menu item differs from the label text, enter the text you want to appear in the Text field.

- Enter a maximum of 255 characters.

- If you do not enter different text, the label text (of the lowest menu level only) will be displayed when the user selects the item.

6 From the Add New Entries selection menu, select an option to determine whether the entry you are defining is added to the top of the current list of selections, the bottom of the list, or before or after the item that is currently selected.

7 Select **Add** to add the item to the list, or select **Modify** to replace the currently selected item with the new label and text.

8 Repeat steps 3 through 7 for as many items as are needed at that menu level.

Generating Trouble Ticket Reports

A set of predefined reports is maintained in a public directory that should be downloaded to your personal configuration directory. Procedure 8.2.8 in Document 611-CD-004-001 *Mission Operation Procedures for the ECS Project* refers to appropriate instructions in the Remedy User's Guide for copying files to share macros and custom reports. These reports are trouble ticket administrative reports generated for local and system-wide usage. There are seven types of predefined reports, including:

- Trouble Ticket Status Report (Summary) – provides a summary of the number of tickets by status.
- Trouble Ticket Status Report (Criteria) – indicates the status of a set of trouble tickets listed on the basis of operator-selected criteria (e.g., by date range, assigned-user, status...).
- Trouble Ticket Status Report (SMC) – provides a summary of the tickets by status for importing into Excel.
- Trouble Ticket Resource Report – indicates by resource the number and type of problems encountered by affected resource.
- Trouble Ticket User Report – indicates by submitter the number and type of trouble tickets in the system.
- Trouble Ticket Statistics Report – indicates statistical information such as mean time to close for a set of trouble tickets listed on the basis of operator-selected criteria.
- Trouble Ticket Priority Report – provides a summary of the number of tickets by priority.

Procedure 8.2.8 in Document 611-CD-004-001 *Mission Operation Procedures for the ECS Project* refers to the Remedy User's Guide, Chapter 5, "Reports" for instructions on working with reports. If you choose to create your own custom report, these instructions provide detailed guidance on selecting report content, setting report layout, specifying the sorting and grouping of report content, generating statistics, setting report options, saving, using, and modifying custom reports, and generating report output.

Suppose you want to print a report on one of the provided custom reports, Trouble Ticket Priority Report. Use the following procedure to create and print the report.

Using a Custom Report

1 From the Trouble Ticket main window in the User Tool, follow menu path **File→Open Query**.

- The **Select Schema - Query** dialog box appears.

2 Select the schema you want to work with by selecting the schema name in the Schema Name list and then selecting the **OK** button, **Return/Enter** key, or by double-clicking on the schema name (in this case, **AR-Help Desk Tickets**).

3 Define the query criteria to be applied to the search by filling in fields in the **Query** window or by using the query bar. (In this case, request all trouble tickets by clearing all fields and leaving the **Query** window blank.)

- The query will return all AR Trouble Tickets.

4 From the Trouble Ticket main window in the User Tool, follow menu path **Query→Report**.

- The **Report** window is displayed.

5 Select the report you want from the **Custom Report Name** list by clicking on the report name (in this case, **Trouble Ticket Priority Report**).

- The **Custom Report Name** list contains all custom report files that are in all directories defined in your AR Path preference.

- The custom report **Trouble Ticket Priority Report** is loaded into the Report window with the report prototype visible. The custom report layout and page setup are applied to the set of trouble tickets defined in the query criteria.

6 Click on the **Print** button in the **Report** window.

- If you have specified the print setup for the report, the report is printed. If you have not yet specified the print setup, the **Print Setup** dialog box appears.

  a) Specify whether you want to use the default printer or a specific printer by selecting one of the radio buttons. If you are using a specific printer, select the printer from the **Specific Printer** drop down list box.

  b) Specify an orientation for the output by selecting either the **Portrait** or **Landscape** radio button.

  c) Select the size and source of the paper.

  d) Select the **OK** button to send your report to the printer.

Performing Operational Work-around

An operational work-around is a temporary modification to operations and user procedures that is entailed by resolution of a trouble ticket. It is characterized by several factors that may affect the way in which procedures are accomplished to conduct operations during the period of temporary inability to conduct operations using normal procedures:

- managed by the ECS Operations Coordinator at each center.
- master list of work-arounds and associated trouble tickets and configuration change requests (CCRs) kept in either hard-copy or soft-copy form for the operations staff.
- hard-copy and soft-copy procedure documents are “red-lined” for use by the operations staff.
- work-arounds affecting multiple sites are coordinated by the ECS organizations and monitored by ECS M&O Office staff.

The work-around is removed when the CCR that corrects the original problem is installed into the operational baseline.

Diagnosing Network Communications Problems

Network problems or faults are failures occurring within the network that prevent the network from meeting its operational objectives. Just as with other problems, management of network faults requires:

- detection of the fault.
- isolation of the fault.
- correction of the fault.

The elements of troubleshooting that support diagnosis of network communications problems are, therefore, essentially the same as those that support other fault diagnosis, and the tools you have learned about for system performance monitoring and troubleshooting are applicable:

- error logs.
- error detection processes.
- diagnostic testing.

Identifying Network Connectivity Problems

Network connectivity problems are indicated by a variety of possible symptoms. These include:

- a user's inability to contact a particular system (e.g., through remote login or file transfer protocol) that had been accessible in the past.
- receipt of an error message that the connection timed out, which could be caused by a system being down, a routing problem, a problem on the default gateway, or bad performance on the network preventing packets from timely passage.
- receipt of an error message indicating an error that the remote system could not be found (e.g., perhaps it is shut off, or it is no longer on the network).

As we have seen, the HP OpenView monitoring tool provides a quick way to detect and identify problems in a network. Its color maps include warnings and indications of major and critical problems with the operational status of elements in the network, including connections between nodes. Therefore, the procedure for looking at HP OpenView network maps for color alerts can help you identify network connectivity problems. If a user or operator is unable to connect to a remote system, a quick check for color alerts can tell you if that system is down. It can also be important to pay attention to the colors of the lines on the map indicating network connections. If you use the HP OpenView default status colors (see Figure 2 on page 12), problems of increasing severity are indicated by a progression of colors as follows:

- cyan -- warning; system faces a potential problem.
- yellow – minor; there is a problem not immediately impeding normal use.
- orange – major; there is a serious problem likely to impede normal use.
- red – critical; there is a severe problem and the affected element is not functioning.

When an operator/user is having problems connecting from one system to another within the same network, a further check for connectivity can be made using HP OpenView Network Node Manager (NNM) and the following procedure to **Ping** the remote system.

Diagnosing Connectivity Problems within a Network

1 On the network map, click on the icon for the remote system.

- The selected icon is highlighted.

2 Follow menu path **Fault→Ping**.

- A window is displayed to show repeated pings. If the remote system is down, the ping will fail. If the ping is successful, repeat steps 1 and 2 for the operator’s/user’s system (from which the connection was originally attempted). If the ping to either system fails, go to step 5. If the ping to both systems is successful, go to step 3.

3 On the network map, click on the icon for the operator’s/user’s originating system, and then click on the icon for the remote system while holding down the **Control** key.

- Both systems are highlighted.

4 Follow menu path **Fault→Remote Ping**.

- A window is displayed to show repeated pings from the originating system to the remote system. If the ping fails, go to step 5. If it is successful, the problem may be in the address mapping between the originating system and the remote system. This can be verified and corrected by using **nslookup** (from a terminal window) to compare the IP address-to-hostname mapping service and IP address for the remote system as seen by the originating system and as it actually is (as seen by another source system).

5 Finally, check for any IP address-to-link address mapping problems by comparing the **Link Address** for the remote system as it is set in the originating system and as it is set in one which is able to communicate with the remote system. To achieve this, select on the map the originating system and also your system. Then, to view the Address Resolution Protocol Cache (ARP Cache) table, follow menu path **Configuration→Network Configuration→ARP Cache**.

- The **ARP Cache** window is displayed for each system selected on the map.
- In the displayed list for the originating system, find the IP Address for the remote system and note its **Link Address**. In the **ARP Cache** window for your workstation, find the IP Address for the remote system in the list and compare its **Link Address** with the one shown in the list for the originating system. If they are not the same, it will be necessary to fix the remote system's link-level address on the originating system. If they are the same, it may be necessary to look for something other than a connectivity problem.

If an operator/user is having difficulty in connecting from a system on one network to a system on a different network, the procedure is somewhat different. If a check of the network map for color alerts determines that the remote system is not down, use the Network Node Manager and the following procedure for further analysis.

Diagnosing Connectivity across Networks

1 On the network map, click on the icon for the remote system.

- The selected icon is highlighted.

2 Follow menu path **Fault→Ping**.

- A window is displayed to show repeated pings. If the remote system or its gateway is down, the ping will fail. If the ping is successful, repeat steps 1 and 2 for the operator's/user's system (from which the connection was originally attempted). If that ping is successful, go to step 5. If the ping to either system fails, go to step 3.

3 On the network map, click on the icon for the gateway to the network with the system for which the ping failed.

- The selected icon is highlighted.

4 Follow menu path **Fault→Ping**.

- A window is displayed to show repeated pings. If the gateway is down, the ping will fail. If the ping is successful, the system for which the ping failed in step 2 is down.

5 On the network map, click on the icon for the operator's/user's originating system, and then click on the icon for the remote system while holding down the **Control** key.

- Both systems are highlighted.

6 Follow menu path **Fault→Locate Route: via SNMP**.

- On the map, the path between the selected systems is highlighted and a window is displayed listing for each node the **Source**, **Source Address**, **Next Hop**, and **Next Hop Address**.
- Verify that the highlighted path is correct; if the route leads to a system other than the one selected, the routing table for the originating system is incorrect. You can view the routing table for each node in turn by clicking on it and then following menu path **Configuration→Network Configuration→Routing Table**.

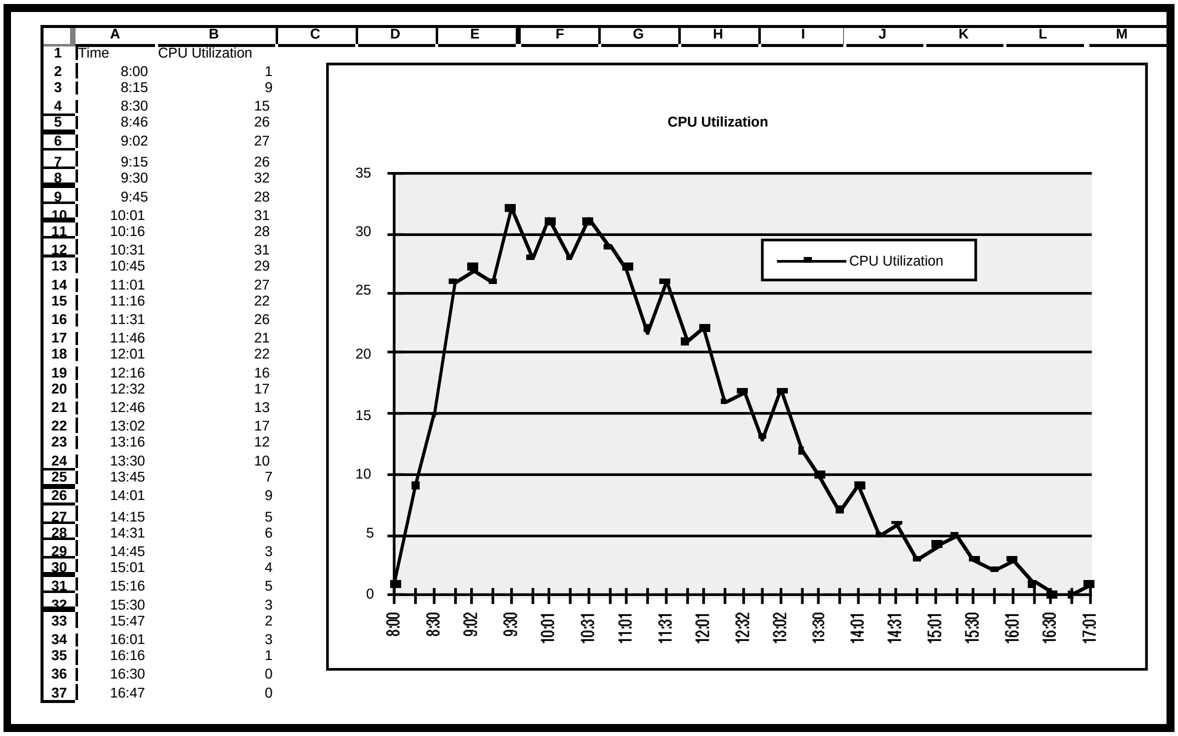
7 Observe the map to verify that all nodes along the correct path are up. A node with yellow or red status indicates that the node either has a problem or is down. If the icon for a node is yellow or red, you need to diagnose the problem on that node.

- If the route is correct and everything is up along the path, it may be necessary to look for something other than a connectivity problem.

Identifying Network Performance Problems

Network performance is more than just a matter of whether the network is functioning or not. Asking whether “normal use” is impeded or not implies an assessment of what is “normal.” If there is a slowdown in the speed of a transaction on the network, perhaps because of high demand, such as an unusually high number of requests being placed on the Science Data Server, users may make a subjective judgment that the performance is not normal. Performance management involves gathering statistics on the operation of the network, maintaining and analyzing logs of the state of the system, and optimizing network operation. If a user concern about the functioning of the system results in a trouble ticket addressing an apparent degradation in the performance of the network, a tools that may help operators/maintainers identify a network performance problem is:

- HP OpenView – permits use of a menu path (e.g., **Performance→CPU Load**, **Performance→Graph SNMP Data→Selected Nodes . . .**) to obtain graphical displays of system performance measures (e.g., interface traffic, CPU usage) on a time line (see example in Figure 8).



	A	B
1	Time	CPU Utilization
2	8:00	1
3	8:15	9
4	8:30	15
5	8:46	26
6	9:02	27
7	9:15	26
8	9:30	32
9	9:45	28
10	10:01	31
11	10:16	28
12	10:31	31
13	10:45	29
14	11:01	27
15	11:16	22
16	11:31	26
17	11:46	21
18	12:01	22
19	12:16	16
20	12:32	17
21	12:46	13
22	13:02	17
23	13:16	12
24	13:30	10
25	13:45	7
26	14:01	9
27	14:15	5
28	14:31	6
29	14:45	3
30	15:01	4
31	15:16	5
32	15:30	3
33	15:47	2
34	16:01	3
35	16:16	1
36	16:30	0
37	16:47	0

Figure 8. Example of HP OpenView Graphical Display of CPU Usage

Diagnosing Network Service Problems

Sometimes it is possible for an operator/user to connect to a remote system, but a command to the remote system is not accepted. For example, a user may try to use a network service (e.g., ftp) from a system on one network to a system on another network, but get an error message. In troubleshooting this problem, the following procedure is applicable.

Diagnosing Network Service Problems

1 On the network map, click on the icon for the remote system.

- The selected icon is highlighted.

2 Follow menu path **Fault→Test IP / TCP / SNMP** to make sure that the selected system supports the network protocols and that the protocols are working.

- A window is displayed to show the results of the test. If there are problems with the protocol, an error will appear in the messages field of the window.
- If the test shows OK, repeat steps 1 and 2 for the originating system. If both systems check out OK, go to step 3.

3 On the network map, click on the icon for the remote system.

- The selected icon is highlighted.

4 Follow menu path **Configuration→Network Configuration→Services** to make sure that the selected system supports the service in question (e.g., **ftp**).

- A window is displayed to show the following information about the selected node:
  - the service protocol: either TCP (Transmission Control Protocol) or UDP (User Datagram Protocol).
  - The port to which the service is bound.
  - The service for which the node is listening (e.g., **ftp**, **telnet**).
- If the test shows OK, repeat steps 1 and 2 for the originating system. If both systems support the service in question, go to step 5. If not, do the following:

  a) Check the file system on the two systems to see if the software for the service (e.g., ARPA Services) is installed. If not, you will have to install the software on the system. If the service software is installed, go to step b.

  b) Configure the service (e.g., ARPA Services) on the system. For HP-UX systems using SAM (System Administration Manager), use the menu path **Configure→HP-UX SAM . . .** to access the SAM tool to configure the service.

  c) Skip step 5 and go to step 6.

5 Check service security on the remote system. Make sure the IP address of the originating system is set for “allow access” and not excluded by a “deny access” in the security files for the service in question (e.g., **/usr/adm/inetd.sec** and **/etc/ftpusers**).

6 Try to use the service again, from the originating system to the remote system, to verify that the problem is resolved.

If there is a problem with network service or performance and you are assigned to work on the trouble ticket, your approach should be a series of systematic steps to diagnose the problem. The steps include:

1. *Review the information in the trouble ticket*. The review gives you insight into the nature of the service problem. For example, if a user experiences a delay in service, such as an apparently too long delay during a request to browse a specified data product using the Search and Order Tool, the description on the trouble ticket describes this system behavior.
2. *Use HP OpenView to see if an alarm has been triggered*. Look for color alerts, and if possible isolate the problem to a particular area of the network.
3. *Use other HP OpenView functions to assist in isolating the problem*. If it is not possible to determine the problem area through color alerts, follow menu path **Locate→Objects** to bring up the map containing a relevant host. For example, review of the trouble ticket for the sample problem mentioned in Step 1 tells you that the problem is with the Science Data Server (SDS), which you know is necessary for a user to browse a specific data product. Using the menu path **Locate→Objects→By Selection Name . . .** can bring up the map containing the SDS managed host.
4. *Use HP OpenView to check the network activity on the host*. Follow menu path **Performance→Network Activity→Interface Traffic**. HP Open View displays an “Interface Traffic” graph containing packets received, packets transmitted, errors received, and errors transmitted. In the sample problem mentioned in Step 1, it is quite possible that the network activity dies not show any sign-on problems or an unacceptable level of activity.
5. *Use HP OpenView to check the CPU load on the host*. Select the managed host (in our example, the SDS host), and follow menu path **Performance→CPU Load**. HP Open View displays a “CPU Load” graph containing the average CPU load on that host. Follow menu path **View→Time Intervals** to bring up a control dialog and scroll back to the time period reported on the trouble ticket for the problem. If there were unusually high numbers of requests during that time period, the CPU Load graph should reflect that high demand. Note, however, that just seeing a high CPU load does not tell you its cause.

Viewing Historical Trends

One of the most useful sources of network troubleshooting information is the history of events leading up to and associated with a problem. To be able to review a history of events, it is necessary to take a proactive view of the system and ensure that data on significant events are monitored and logged. The HP OpenView tool Network Node Manager provides several capabilities to facilitate proactive monitoring of the network, including:

- data collection.
- event configuration.
- application building (for applications to do the monitoring).

The initial set-up or full configuration for effective monitoring of the network can require several weeks to achieve, but it is well worth the attention required to establish a monitoring approach that will require little from you to administer but will provide useful troubleshooting data when it is needed. The set-up process for monitoring with HP OpenView entails several steps which you will want to accomplish in the first few weeks of your network management activities:

- establish baselines for normal network performance.
- build applications to monitor trends.
- set up thresholds for monitored Management Information Base (MIB) values.
- refine the thresholds.
- set up event-triggered actions.

Establishing Baselines for Normal Network Performance

Establishing a baseline requires checking the condition of the network over a period of time. To accomplish this, it is necessary to select information to look at, and then monitor it during the course of several days or weeks. Suppose, for example, that you are interested in the Maintenance and Operations segment and wish to collect data on the SSI&T Workstations. The following procedure is applicable.

Establishing Baselines for Normal Network Performance

1 Follow menu path **Options→Data Collection & Thresholds: SNMP**.

- A dialog box titled **is Data Collection & Thresholds: SNMP** is displayed.
- If the MIB object on which you want to collect data is already displayed in the **MIB Objects** list in the dialog box, click on that object. [NOTE: The enterprise-specific Management Information Base (MIB) for which you want to collect data must be loaded into the Loaded MIB database. For ECS installations, this has been done for you, and the objects will appear. If a new object has been added to the network, and you want to collect data on it, see *HP OpenView, Using Network Node Manager*, “Loading MIBs” in the chapter on Managing MIB Data.] For this example, if you are interested in monitoring traffic on the hub and printer nodes, you may wish to monitor the following MIB objects:
  - **.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets**.
  - **.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets**.

2 Click on **.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets** and then follow menu path **Edit→Add→MIB Collections**.

- The **Data Collection & Thresholds/Add Collection for *xxxxx*** dialog box is displayed.

3 Add the source name (the name or IP address of the node on which you want to collect data), either by entering the name in the **Source** field and clicking on the **Add** button, or by selecting the node(s) (for this example, select the AIT workstations) on the network map and clicking on the **Add From Map** button.

- The **List of Collection Sources** list area shows the name(s) of the selected node(s).
- Repeat this step to add other names to the **List of Collection Sources** as desired.

4 Specify the collection mode using the **Collection Mode** option button and choosing one option from its option menu.

- The four choices on the **Collection Mode** option menu are “**Exclude Collection**” (a way of excluding certain devices from a wildcard list, which may be specified in Step 3), “**Store, Check Thresholds**,” “**Store, No Thresholds**,” and “**Don’t Store, Check Thresholds**.” For example, select “**Store, No Thresholds**.”

5 Specify a polling interval in the **Polling Interval** field by entering a positive real number followed by an "**s**," "**m**," "**h**," "**d**," "**w**," or "**y**," indicating seconds, minutes, hours, days, weeks, or years, respectively. For example, enter "**1h**" to poll at hourly intervals.

WARNING

A collection with a short polling interval can easily fill up a disk. Be aware of the current collection configuration.

6 Specify the MIB instance of the object on which you want to collect data. To do this, click on the option button and select the **All** option.

- The options are "**All**" instances of the MIB object, "**From List**" as specified in the input box, and "**From Regular Expression**" as specified in the input box.

7 Click on the **OK** button. The **Data Collection & Thresholds/Add Collection** dialog box disappears and the MIB object(s) is/are added to the selection list of MIB objects configured for collection in the **MIB Data Collection** dialog box.

8 Repeat steps 2 through 7, except in step 2 click on **.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets**.

9 Check to see if data are being collected by observing the status (**Collecting** or **Suspended**) listed in the **MIB Data Collection** dialog box.

- If the status of the MIB object(s) is **Suspended**, change it to collecting by selecting (highlighting) the object(s) and following menu path **Actions**→**Resume Collection**.

10 Implement the change and begin collection by following menu path **File**→**Save**.

NOTE: Even though the status entry shows a change when you follow menu path **Actions**→**Resume Collection**, the change does not take effect until you perform the **File**→**Save** operation.

Building Applications to Monitor Trends

You can use HP OpenView to build applications without programming to display collected MIB data. These applications can be integrated into the HP OpenView menu structure for ease of use. For example, to graph the data collected on your selected workstations, the following procedure is applicable.

Building an Application to Monitor Trends

1 Follow menu path **Options→MIB Application Builder: SNMP**.

- The **MIB Application Builder:SNMP** dialog box is displayed.

2 Follow menu path **Edit→Add MIB Application . . .** .

- The **Add MIB Application** dialog box is displayed.

3 Type the name of the application (e.g., in this case, **SSTraffic**) in the **Application ID** field.

- This field determines the name of the file where the application information is to be stored (in the $OV_REGISTRATION/C/ovmib/ directory); therefore, each application must have a unique name.

4 Select the type of application you want to build by clicking on the **Application Type** option button.

- There are three options for application type: **Form**, **Table**, and **Graph**. For this example, select **Graph**.

5 Enter the title of your application (e.g., **SSIT Traffic**) in the **Application Title** field.

- This title appears in the menu path (e.g., **Performance→Graph SNMP Data→ SSIT Traffic**) and in the title bar of the dialog box when the application is run.

6 Click on the **Add** button of the **Add MIB Application** dialog box.

- The **MIB Application Builder/Add MIB Objects** dialog is displayed.

7 Specify the MIB object to include in your application (in this case, **.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets**).

- The specification may be done in either of two ways: 1) navigate the MIB tree and select the desired object, or 2) type in the MIB object in the **MIB Object ID** field.

8 Click on the **Apply** button.

- The MIB object is added to the **Display Fields** window of the **Add MIB Application** dialog box and the **MIB Application Builder/Add MIB Objects** dialog box remains displayed.

9 Repeat Steps 7 and 8 to specify additional MIB objects to include in your application (in this case, **.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets**).

- In Step 8, after the specification of the last MIB object to be included, you may click on the **OK** button (instead of the **Apply** button). In this case, the MIB object is added to the **Display Fields** window of the **Add MIB Application** dialog box and the **MIB Application Builder/ Add MIB Objects** dialog box is closed. If you do not use the **OK** button, when finished you will have to exit the **MIB Application Builder/ Add MIB Objects** dialog box by clicking on the **Cancel** button.

10 Optionally, edit the **Label** for each MIB object selected.

- The default is the last component of the MIB object name; when a MIB object in the **Display Fields** window is highlighted, this last component appears in the **Label** field, where you may edit it and implement the edits by clicking on the **Replace** button.

11 Optionally, change the order of the items in the list by selecting an item to move and clicking on the **Up** or **Down** arrows to the right of the **MIB Object ID** list; each click moves the item up or down one position.

- Changing the order affects the order in which the items are displayed when you run the application.

12 To make the application appear in the HP OpenView menu hierarchy, enter the menu path in the **Menu Path** input box of the **Add MIB Application** dialog box.

- Use the character sequence **->** to separate menu items in the cascaded path.

13 Enter the OVW selection rule in the **Selection Rule** field.

- The default selection rule is based on defined HP OpenView capabilities of the nodes for which the application is compatible; components of the rule are separated by "||" to indicate logical "or" or "&&" to indicate logical "and."

- If the application is registered in the menu bar (Step 12), the menu item for this application is only accessible if the capabilities of the selected nodes match those defined in this selection rule. For our example, if the selection rule is specified as **(isSNMPsupported)||(is SNMPProxied)&&(isNode)&&isWorkstation)**, then the menu choice will be grayed out unless the selected node is a workstation that is SNMP supported or proxied.

14 Enter any help text that you want displayed for your application.

- When you create the MIB operation menu item, the program automatically adds an entry accessible through menu path **Help→Index→Function** and in the dialog box accessible by clicking on the **Help** button.

15 Click on the **OK** button.

- The new MIB application is created and the **Add MIB Application** dialog box is closed.

Once you have collected data for a suitable period of time to observe trends (e.g., two weeks), you can review the data. One powerful tool for viewing historical data is the HP OpenView Grapher. We have already seen an example of using an HP OpenView graph, *viz.*, to view CPU load. The HP OpenView Grapher assists the review of historical trends in several ways, permitting:

- the organization and viewing of collected information in graph form.
- the graphing of combinations of data values in the same graph.
- viewing data values representing different instances of data variables or different variables for different nodes.
- viewing data for selected nodes or viewing all the data in the Data Collector database.

Before accessing the Grapher, data collection on the nodes of interest must have been started by using menu path **Options→SNMP Data Collection & Thresholds**, as just described. Then, when the Grapher is started, all the collected data from the selected nodes will be read into memory and will be available for browsing with the Grapher functions, using the following procedure.

Viewing Historical Trends using HP OpenView Grapher

1 On the network map, click on the icon(s) for the node(s) of interest.

- The selected icon is highlighted.

2 Follow menu path **Performance→Graph SNMP Data→Selected Nodes**.

- The primary window for the HP OpenView Graph tool is displayed.
- The **Graph Selected Nodes** dialog box is displayed. It is a line graph with a legend across the top of the graph to identify the graphed data and time shown on the X-axis.

3 Manipulate the graph to obtain the desired display.

- Available manipulations include **selecting time intervals**, **zoom, modifying line attributes**, and **resizing the graph window**.

After you have collected and reviewed data for a period of time, you may wish to define thresholds for monitored numeric MIB values. This permits you to set limits on the collection of data such that an event record is made only when the monitored value exceeds established boundary conditions. Suppose, for example, that you have monitored and reviewed traffic on the hub for two weeks, and you believe that the traffic during that time is representative of typical traffic during normal operations. You note the maximum value for inbound octets (**ifInOctets**) during that period, and decide that for monitoring hub traffic you want to have an event recorded only if that value is exceeded. You want to set the threshold at that level, and to set a rearm value of 10 percent of the threshold value. (NOTE: The rearm value controls how frequently a threshold event is generated by the data collector. When the MIB value satisfies the **Rearm** expression, a rearm event is generated. Another threshold event will not be generated until the rearm event occurs and the collected value subsequently satisfies the **Threshold** expression.) The following procedure is used.

Defining Thresholds and Rearm Values

1 Follow menu path **Options→Data Collection & Thresholds: SNMP**.

- A dialog box its title is **Data Collection & Thresholds: SNMP** is displayed.

2 From the **MIB Objects Configured for Collection** selection list, select the item for which you want to set thresholds.

- The details for that item appear in the lower section of the dialog box, **MIB Collection Summary**.

3 Select the source from the **MIB Collection Summary** list.

- You may select multiple items.

4 Follow menu path **Edit→Modify→MIB Collections**.

- The **Data Collection & Thresholds, Modify Collection** dialog box is displayed.

5 Select either **Don't Store, Check Thresholds** or **Store, Check Thresholds** from the option menu next to the Collection Mode label.

- The **Threshold** and **Rearm** fields are un-grayed and made available.

6 Specify a polling interval in the **Polling Interval** field by entering a positive real number followed by an "**s**," "**m**," "**h**," "**d**," "**w**," or "**y**," indicating seconds, minutes, hours, days, weeks, or years, respectively. For example, enter "**1h**" to poll at hourly intervals.

WARNING

A collection with a short polling interval can easily fill up a disk. Be aware of the current collection configuration.

7 Specify a **Specific Event** (i.e., trap) number.

- The default **Specific Event** (58720263) is the enterprise-specific trap that the data collector sends when a threshold or rearm value is exceeded. When you are customizing a data collection, you can assign your own trap number, using an odd number between 1001 and 1999. (The even numbers 1002 to 2000 are reserved for the respective rearm trap IDs, which are generated automatically by HP Open View.) For this example, specify **1901** as the trap number.

- The data collector sends the trap using the Enterprise ID of the Management Station.

- The default trap is logged in the **Threshold Events** category in the **Events** notification window.

- The exact trap number allows you to perform a specific action when this kind of threshold value is passed or rearmed.

8 Enter the threshold value (in this case, ***TBD***) in the **Threshold** field.

- Use this field when you want to be notified of data patterns that are outside normal expectations. When the threshold value is passed, the specified event is generated, and the **Event Categories** window notifies you accordingly.

9 Enter a rearm value (in this case, ***TBD***) in the **Rearm** field and click on the appropriate toggle button to specify whether the entered value is **Absolute** or a **Percent** of the threshold value.

- The **Rearm** value is used to avoid continuous generation of events while a collected value exceeds the threshold value. When the MIB Object value drops below, or is equal to, the **Rearm** value, a **Rearm Event** is generated. Another **Threshold Event** will not occur until the **Rearm Event** is generated and the MIV Object value again exceeds the threshold setting.

10 Optionally, specify a value for the **Consecutive Samples** field.

- This value specifies the number of consecutive times the **Threshold** expression must be satisfied before a corresponding event is generated.

11 Specify on which instance of the MIB Object you want to collect data.

12 Click on the **Apply** button to remain in the dialog box, or click on the **OK** button which will exit the **Data Collection & Thresholds** dialog box.

- The new collection parameters are initiated.

Refining Thresholds

Once you have monitored your system for a time using thresholds, you will have a basis for assessing the appropriateness of the thresholds you set. You may note one of at least two possible conditions that suggest resetting the threshold and rearm values:

- you are receiving several threshold events in the course of a day without any apparent loss in network performance (e.g., hub traffic is high enough to exceed the set thresholds, but everyone finds their printing needs satisfied without trouble).

- you are experiencing network performance problems but are not receiving threshold events that might give you advance warning of those problems (e.g., there are large backlogs that cause people to have to wait excessively long for print jobs, but the hub and printer traffic are not sufficient to cause threshold events).

To refine your thresholds, the following procedure is applicable.

Refining Thresholds for MIB Data Collection

1 On the map, select the node for which you want to change the threshold/rearm value (e.g., select the printer hub).

2 Follow menu path **Options→Data Collection & Thresholds: SNMP**.

- The **MIB Data Collection** dialog box appears (its title is **Data Collection & Thresholds: SNMP**).

3 From the **MIB Objects Configured for Collection** selection list, select the item for which you want to reset thresholds.

- The details for that item appear in the lower section of the dialog box, **MIB Collection Summary**.

4 Select the source from the **MIB Collection Summary** list.

- You may select multiple items.

5 Follow menu path **Edit→Modify→MIB Collections**.

- The **Data Collection & Thresholds, Modify Collection** dialog box is displayed.

6 Enter the new threshold value (in this case, ***TBD***) in the **Threshold** field.

- When the threshold value is passed, the specified event is generated, and the **Event Categories** window notifies you accordingly.

7 Enter a rearm value (in this case, ***TBD***) in the **Rearm** field and click on the appropriate toggle button to specify whether the entered value is **Absolute** or a **Percent** of the threshold value.

- When the MIB Object value drops below, or is equal to, the **Rearm** value, a **Rearm Event** is generated. Another **Threshold Event** will not occur until the **Rearm Event** is generated and the MIV Object value again exceeds the threshold setting.

8 Optionally, once you have fine tuned the threshold settings, you may want to turn off the data storage function, but continue to check for thresholds. To do this set the data collection mode to **Don't Store, Check Thresholds** by selecting that option from the option menu next to the Collection Mode label.

9 Click on the **Apply** button to remain in the dialog box, or click on the **OK** button which will exit the **Data Collection & Thresholds** dialog box.

- The new collection parameters are initiated.

Setting Up Event-Triggered Actions

Once you have attained stability in threshold settings, you may find it desirable to set up an action to occur when one of the threshold values is exceeded. For example, you may wish to have a pop-up window appear to notify you with a message and, perhaps, with an audible signal upon occurrence of SSI&T Workstation traffic in excess of your set threshold. Use the following procedure.

Event Configuration

1 Open the **Event Configuration** dialog box by following menu path **Options→Event Configuration**.

- The **Event Configuration** dialog box is displayed.

2 Select the item in the **Enterprise Identification** list which corresponds to the event you want to configure (e.g., select SNMP).

- Defined events for that Enterprise Identification appear in the **Event Identification** list.

3 Follow menu path **Edit→Add→Event**.

- The **Event Identification/Add Event** dialog box is displayed.

4 Enter a unique event name (this name cannot contain embedded spaces) in the **Event Name** field (e.g., enter **SSIT_High** to indicate SSI&T Workstation Traffic High).

5 Use the option button and associated menu to select the generic trap type. For this example, select **Enterprise Specific**.

6 In the **Specific Trap** field, which is displayed only when you have selected the **Enterprise Specific** option for generic trap type, enter the specific number of the trap.

- In this case, specify **1901** (The trap ID you choose here must be the same as the one you set up in the data collection and threshold specification).

7 In the **Event Description** field, enter any text description you want to provide to characterize the meaning of the event.

8 In the **Event Sources** field, enter the sources (nodes) for which the event applies, or select the sources on the map and click on the **Add from Map** button.

9 Use the **Event Category** option button to select the category in which to display notification of the event.

- Select **Threshold Events**. If you select “Log Only” or “Don’t Log or Display,” the event will not be displayed in the Event Log Browser.

10 Use the **Severity** option button to select the severity of the event.

- For this example, select **Warning** as the severity level appropriate for exceeding the threshold.

11 In the **Event Log Message** field, leave the default message. This message will appear in the event notification window when the event is received.

12 In the **Popup Notification** field, type the message which you want to appear in the popup window when the event occurs (e.g., "**SSI&T traffic threshold exceeded; check Event Log Browser for details.**").

12 Leave the **Command** field blank. This field can be used to specify a command and corresponding arguments to be performed automatically upon occurrence of the event.

13 Follow menu path **File**→**Save** and save the event.

Although the foregoing procedures can be used to define data collection and configure events, the developers of ECS have provided data collection definitions for a variety of system errors or unusual events for you. They have been configured to poll every 15 minutes and to provide a popup notification if event occurrences (i.e., errors or unusual events) exceed a threshold, typically 5 or 10 percent of attempted messages or transmissions. Table 1 lists the types of data collection and event configurations that have been provided.

Table 1
ECS MIB Data Collection Definitions

MIB Object Group	Resource/Expression
ICMP	ICMP%InErrors
	ICMP%InDestUnreachs
	ICMP%OutErrors
	ICMP%OutDestUnreachs
TCP	TCP%InErrors
UDP	UDP%InErrors
IP	IP%InHdrErrors
	IP%InAddrErrors
	IP%InUnknownProtos
	IP%InDiscards
	IP%OutDiscards
	IP%OutNoRoutes
Network Interface	If%InDiscards
	If%InErrors
	If%InUnknownProtos
	if%OutDiscards
	If%OutErrors

Using the Event History Log Browser

Another ECS tool of use for reviewing events at or near the time of a problem is HP OpenView **Event History Log Browser**. When a popup notification is received, or to review details of events indicated by a color alert in the HP OpenView **Event Categories** window, you can examine the listings in this browser. To use this HP OpenView tool, select the managed host (e.g., the SSI&T host) and enter the initial time to be near, but prior to, the time the problem is known to have occurred. Use the following procedure.

Using HP OpenView Event History Log Browser

1 Follow menu path **Fault→Event**.

- The **All Events Browser** window is displayed.

2 Follow menu path **View→Set Filters . . . .**

- The **Filters** window is displayed.

3 Click on the toggle button for **Match By Time**.

- A time **scroll bar** appears: use the slider to set the initial time.

4 On the network map, click on the managed host (e.g., **ait*x*1sun**).

- The selected icon is highlighted.

5 Click on the toggle button for **Match Source**.

- A source **text window** appears with text entry field and buttons.

6 Click on the **Add From Map** button.

- The source identifier appears in the text window.

7 Click on the **Apply** button.

- The Event History Log Browser displays the events from **ait*x*1sun** in the selected time period.

This page intentionally left blank.

Practical Exercise

Introduction

This exercise is designed to practice key elements of the System Troubleshooting procedures. Perform the tasks identified in the exercise.

Equipment and Materials

One ECS workstation, a copy of 609-CD-003-001 *Operations Tools Manual*, and a copy of 611-CD-004-001 *Mission Operations Procedures for the ECS Project*.

Perform Activities Related to System Monitoring and Troubleshooting

1. Use ECS tools to perform system monitoring activities, including HP OpenView maps and event log files for checking the health and status of the network and the web browser to access the EBnet Web Page.

2. Use HP OpenView to check for event notifications, and browse the event logs for several event categories as you would to diagnose a problem event.

3. Add a user to Remedy. Then change that user's privileges in two ways: first, change the group to which the user is assigned; then, change the access privileges of the group to which you last assign the user.

4. Follow Procedure 8.2.7 in Document 611-CD-004-001 *Mission Operation Procedures for the ECS Project* and use the Remedy Admin Tool to add a key word to the **RelB-Menu-Key Words** pull-down pick-list in the RelB-Trouble Ticket schema.

5. Use HP OpenView Network Node Manager and configure the system to collect data on a network node, using thresholds and rearm values.

This page intentionally left blank.

Slide Presentation

Slide Presentation Description

The following slide presentation represents the slides used by the instructor during the conduct of this lesson.

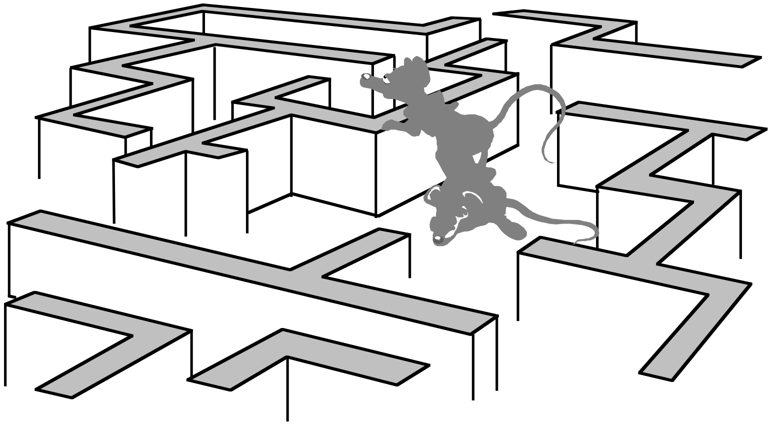
This page intentionally left blank.

SYSTEM TROUBLESHOOTING

ECS Version 2.0 Training

Overview of Lesson

- Introduction
- System Troubleshooting Topics
  - System Performance Monitoring
  - Problem Analysis/Troubleshooting
  - Trouble Ticket (TT)
  - Diagnosing Network Communications Problems
- Practical Exercise



Objectives

- **Overall: Proficiency in methodology and procedures for system troubleshooting for ECS**
  - **Conduct system performance monitoring**
  - **Perform problem analysis and troubleshooting**
  - **Set up trouble ticket users and configuration**
  - **Diagnose network communications problems**

Importance

Lesson helps prepare several ECS roles for effective system troubleshooting, maintenance, and problem resolution:

- **DAAC Computer Operator, System Administrator, and Maintenance Coordinator**
- **SEO System Administrator, System Engineer, System Test Engineer, and Software Maintenance Engineer**
- **DAAC System Engineers, System Test Engineers, Maintenance Engineers**

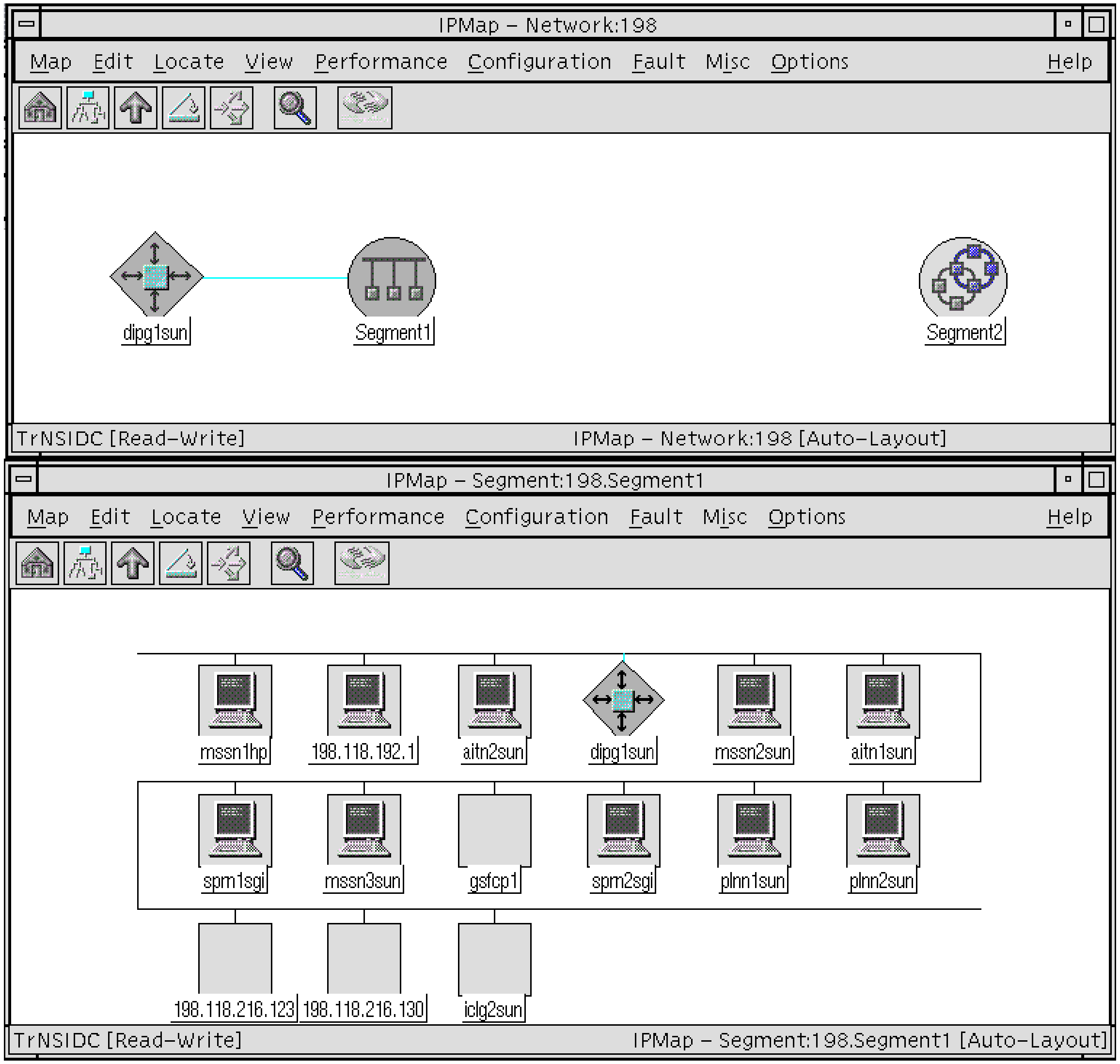
System Performance Monitoring

- Maintaining Operational Readiness
  - System operators -- close monitoring of progress and status
    - Notice any serious degradation of system performance
  - System administrators and system maintenance personnel -- monitor overall system functions and performance
    - Administrative and maintenance oversight of system
    - Watch for system problem alerts
    - Use monitoring tools to create special monitoring capabilities
    - Check for notification of system events

Checking Network Health & Status

- HP Open View system management tool
  - Site-wide view of network and system resources
  - Status information on resources
  - Event notifications and background information
  - Operator interface for managing resources
- HP Open View monitoring capabilities
  - Network map with color alerts to indicate problems
  - Indication of network changes
  - Creation of submaps for special monitoring
  - Event notifications

HP Open View Network Maps


IPMap – Network:198
Map Edit Locate View Performance Configuration Fault Misc Options Help
dipg1sun
Segment1
Segment2
TrNSIDC [Read-Write]
IPMap – Network:198 [Auto-Layout]
IPMap – Segment:198.Segment1
Map Edit Locate View Performance Configuration Fault Misc Options Help
mssn1hp
198.118.192.1
aitn2sun
dipg1sun
mssn2sun
aitn1sun
spm1sgi
mssn3sun
gsfcp1
spm2sgi
plnn1sun
plnn2sun
198.118.216.123
198.118.216.130
iclg2sun
TrNSIDC [Read-Write]
IPMap – Segment:198.Segment1 [Auto-Layout]

Network Discovery and Status

- HP OpenView discovers and maps network and its elements
  - Configured to display status
  - Network maps set for read-write
  - IP Map application enabled
- HP OpenView Network Node Manager start-up
  - Network management processes must be running
    - ovwdb, trapd, ovtopmd, ovactiond, snmpCollect, netmon
  - Check using command: ovstatus
- Status categories
  - Administrative: Not propagated
  - Operational: Propagated from child to parent
- Compound Status: How status is propagated

HP OpenView Default Status Colors

Status Condition	Symbol Color	Connection Color
Unmanaged (a)	Off-white	Black
Testing (a)	Salmon	Salmon
Restricted (a)	Tan	Tan
Disabled (a)	Dark Brown	Dark Brown
Unknown (o)	Blue	Black
Normal (o)	Green	Green
Warning (o)	Cyan	Cyan
Minor/Marginal (o)	Yellow	Yellow
Major (o)	Orange	Orange
Critical (o)	Red	Red

(a) Administrative Status (o) Operational Status

Monitoring: Check for Color Alerts

- Open a map
- Compound Status set to default
- Color indicates operational status
- Follow color indication for abnormal status to isolate problem

Monitoring: Check for New Nodes

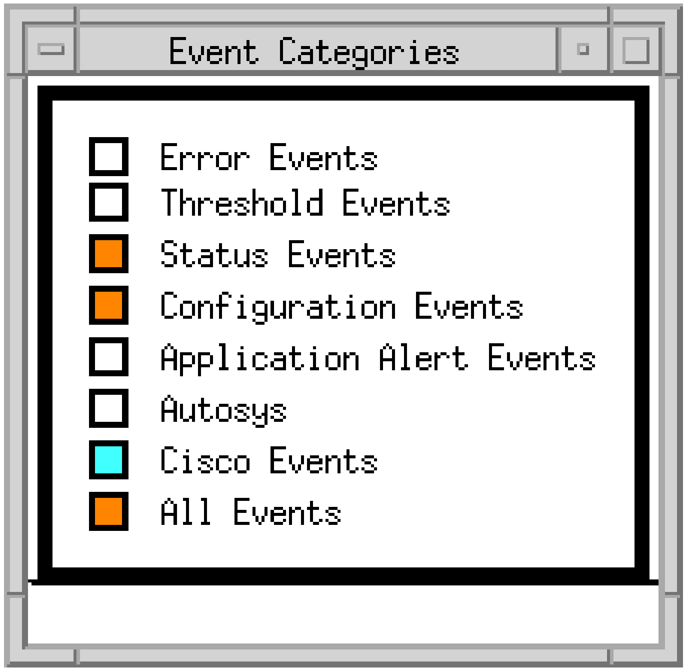
- IP Map application enabled
  - Automatic discovery of IP-addressable nodes
  - Creation of object for each node
  - Creation and display of symbols
  - Creation of hierarchy of submaps
    - Internet submap
    - Network submaps
    - Segment submaps
    - Node submaps
- Autolayout
  - Enabled: Symbols on map
  - Disabled: Symbols in New Object Holding Area

Monitoring: Special Submaps

- Logical *vs*. physical organization
- Create map tailored for special monitoring purpose
- Two types and access options
  - Independent of hierarchy, opened by menu and dialog
  - Child of a parent object, accessible through symbol on parent

Monitoring: Event Notifications

- Event: a change on the network
  - Registers in appropriate Events Browser window
  - Button color change in Event Categories window
- Event Categories
  - Error events
  - Threshold events
  - Status events
  - Configuration events
  - Application alert events
  - All events



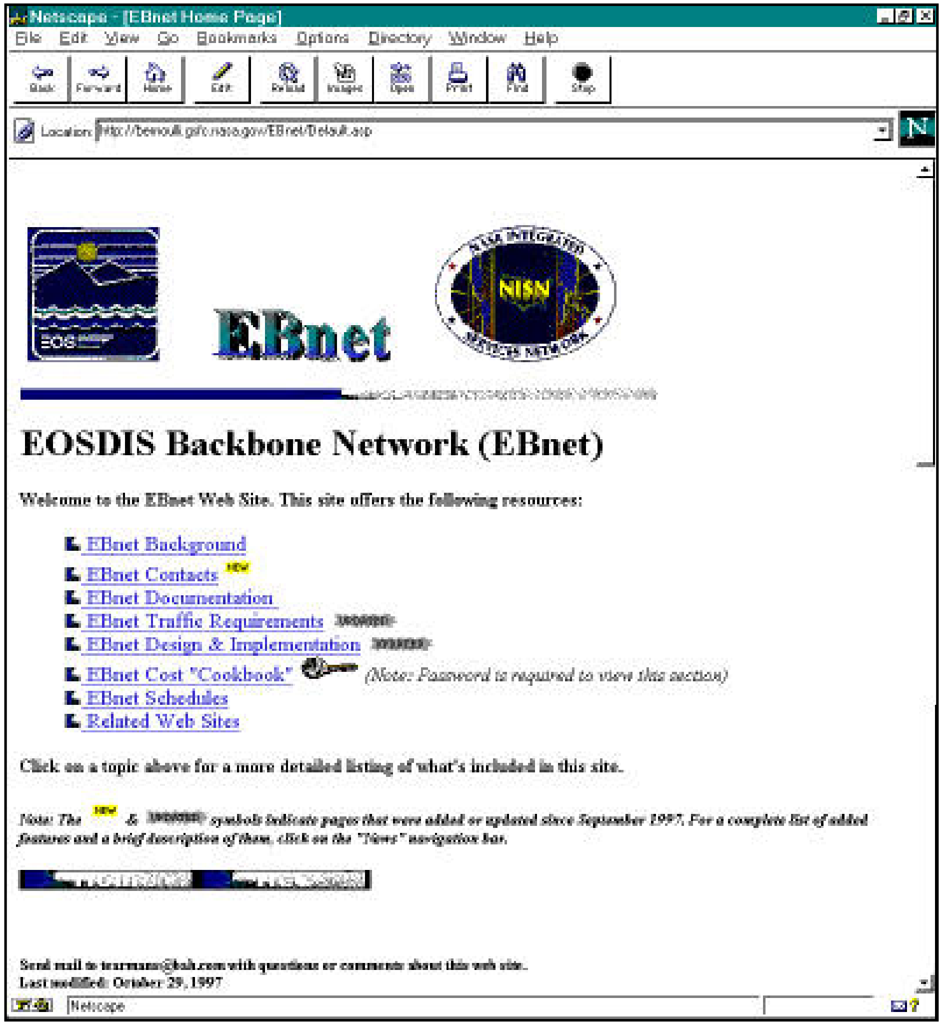
Event Categories

□ Error Events
□ Threshold Events
🟧 Status Events
🟧 Configuration Events
□ Application Alert Events
□ Autosys
🟦 Cisco Events
🟧 All Events

Accessing the EBnet Web Page

- EBnet is a WAN for ECS connectivity
  - DAACs, EDOS, and other EOSDIS sites
  - Interface to NASA Science Internet (NSI)
  - Transports spacecraft command, control, and science data
  - Transports mission critical data
  - Transports science instrument data and processed data
  - Supports internal EOSDIS communications
  - Interface to Exchange LANs
- EBnet home page URL
  - http://bernoulli.gsfc.nasa.gov/EBNET/

EBnet Home Page


Netscape - [EBnet Home Page]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Location: http://bernoulli.gsfc.nasa.gov/EBnet/Default.asp
EOS
EBnet
NASA INTEGRATED SERVICES NETWORK
NISN
Netscape

EOSDIS Backbone Network (EBnet)

Welcome to the EBnet Web Site. This site offers the following resources:

- EBnet Background
- EBnet Contacts NEW
- EBnet Documentation
- EBnet Traffic Requirements UPDATED
- EBnet Design & Implementation UPDATED
- EBnet Cost "Cookbook" *(Note: Password is required to view this section)*
- EBnet Schedules
- Related Web Sites

Click on a topic above for a more detailed listing of what's included in this site.

Note: The NEW & UPDATED symbols indicate pages that were added or updated since September 1997. For a complete list of added features and a brief description of them, click on the "News" navigation bar.

Send mail to tearmann@bah.com with questions or comments about this web site.
Last modified: October 29, 1997

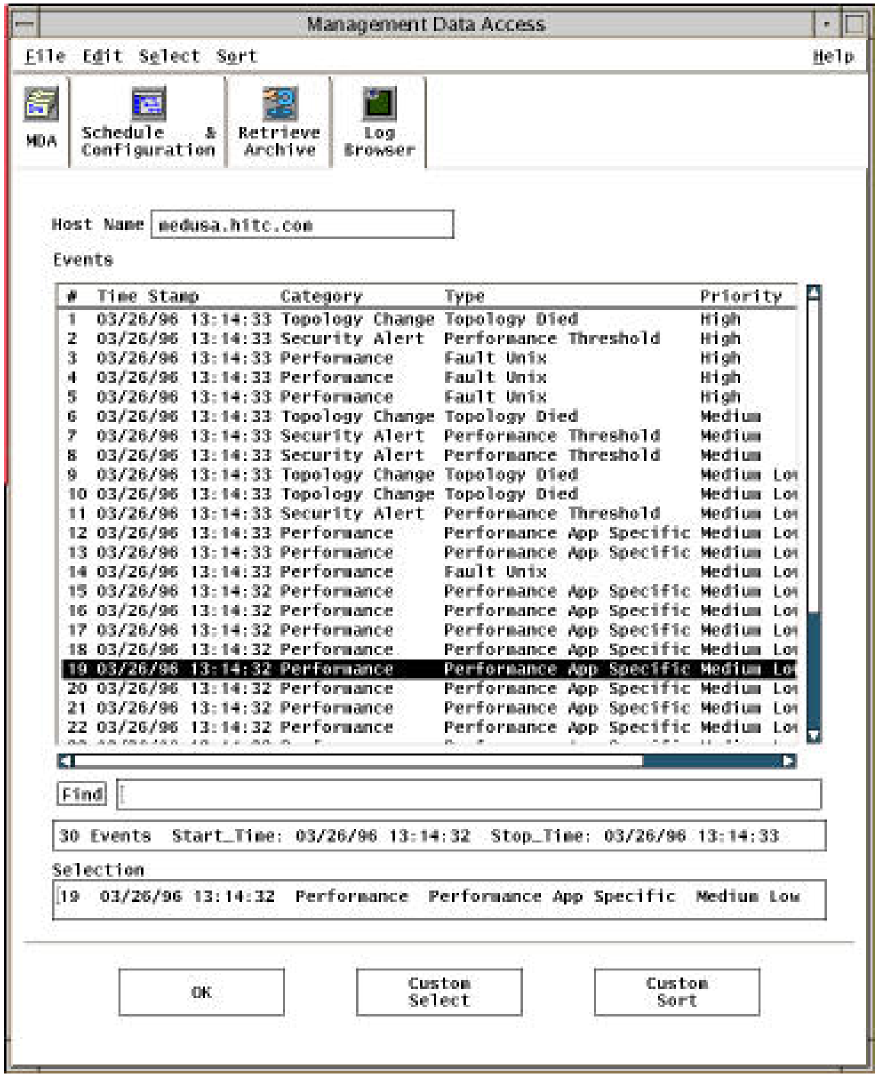
Analysis/Troubleshooting: System

- **COTS product alerts and warnings**
  (e.g., HP OpenView, AutoSys/Xpert, Tivoli)
- **COTS product error messages and event logs**
  (e.g., HP OpenView, Tivoli, ClearCase®)
- **ECS Custom Software Error Messages**
- **Management Data Access (MDA) Services**
  (Event Log Browser)
  - **Single log for all significant system events**
  - **Created by MSS agent**
  - **Open, sort, filter, and browse logged events**
    - **Select a log file**
    - **Filter events**
    - **Sort events**
    - **View event fields for details**

ECS Event Priorities

- *Low* -- informational events that do not have adverse operational impact
- *Medium-Low* -- warnings or recoverable errors that are of low significance
- *Medium* -- indication of potential problems, or abnormal system activity but system remains operational
- *High* -- error event with impact on operations; abnormal event that is fatal to, or seriously degrades operations

MDA Event Log Browser



Host Name medusa.hitc.com

Events

#	Time Stamp	Category	Type	Priority
1	03/26/96 13:14:33	Topology Change	Topology Died	High
2	03/26/96 13:14:33	Security Alert	Performance Threshold	High
3	03/26/96 13:14:33	Performance	Fault Unix	High
4	03/26/96 13:14:33	Performance	Fault Unix	High
5	03/26/96 13:14:33	Performance	Fault Unix	High
6	03/26/96 13:14:33	Topology Change	Topology Died	Medium
7	03/26/96 13:14:33	Security Alert	Performance Threshold	Medium
8	03/26/96 13:14:33	Security Alert	Performance Threshold	Medium
9	03/26/96 13:14:33	Topology Change	Topology Died	Medium Low
10	03/26/96 13:14:33	Topology Change	Topology Died	Medium Low
11	03/26/96 13:14:33	Security Alert	Performance Threshold	Medium Low
12	03/26/96 13:14:33	Performance	Performance App Specific	Medium Low
13	03/26/96 13:14:33	Performance	Performance App Specific	Medium Low
14	03/26/96 13:14:33	Performance	Fault Unix	Medium Low
15	03/26/96 13:14:32	Performance	Performance App Specific	Medium Low
16	03/26/96 13:14:32	Performance	Performance App Specific	Medium Low
17	03/26/96 13:14:32	Performance	Performance App Specific	Medium Low
18	03/26/96 13:14:32	Performance	Performance App Specific	Medium Low
19	03/26/96 13:14:32	Performance	Performance App Specific	Medium Low
20	03/26/96 13:14:32	Performance	Performance App Specific	Medium Low
21	03/26/96 13:14:32	Performance	Performance App Specific	Medium Low
22	03/26/96 13:14:32	Performance	Performance App Specific	Medium Low

30 Events Start_Time: 03/26/96 13:14:32 Stop_Time: 03/26/96 13:14:33

Selection

19 03/26/96 13:14:32 Performance Performance App Specific Medium Low

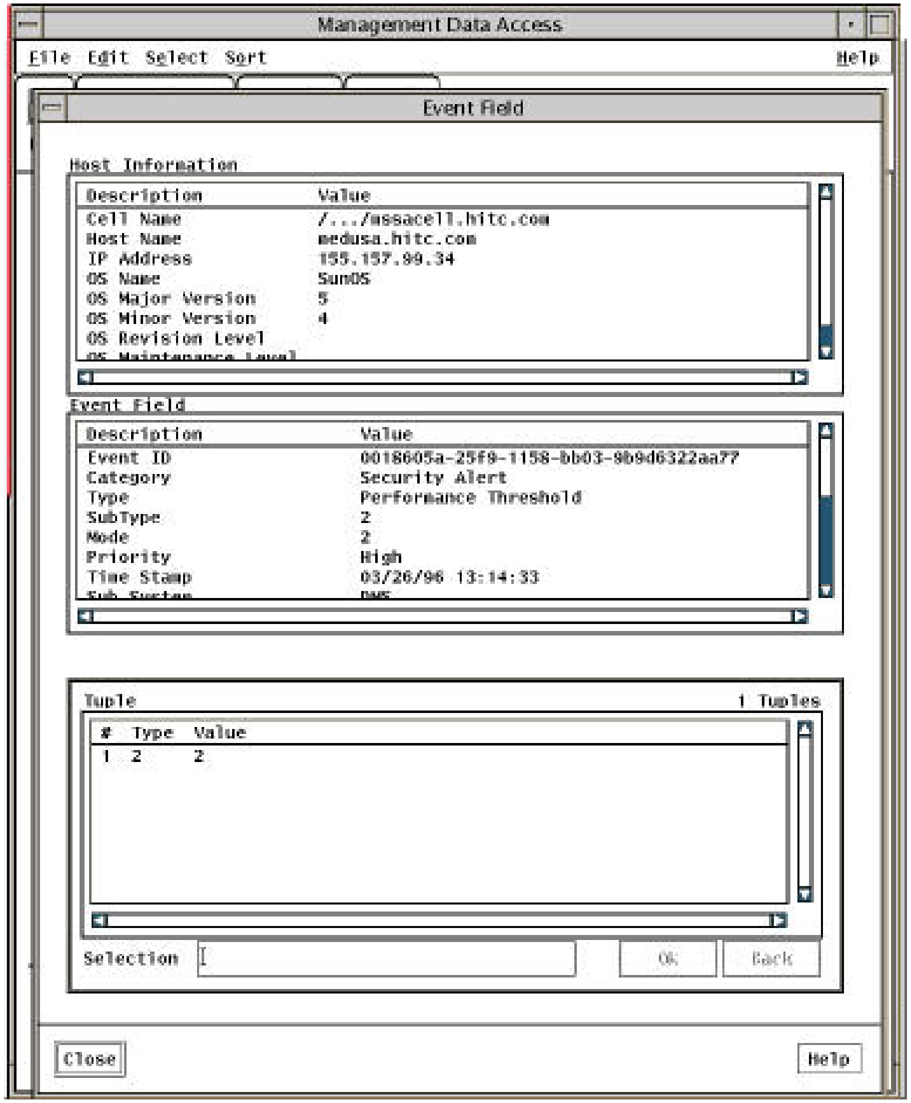
Systematic Troubleshooting

- Thorough documentation of the problem
  - Date/time of problem occurrence
  - Hardware/software
  - Initiating conditions
  - Symptoms
- Verification
  - Identify/review relevant publications (e.g., COTS product manuals, ECS tools and procedures manuals)
  - Replicate problem
- Identification
  - Review product/subsystem logs
  - Review ECS error messages, MDA Event Log Browser
- Analysis
  - Detailed event review (e.g., MDA Event Log Browser Event Fields)
  - Determination of cause/action

Log Browser Detailed Event Fields

- **Performance Metrics**
  - – **Measured Values (e.g., time, number of elements, rate)**
- **Tuples**
  - – **Monitored Data Strings (e.g., name, identifying numbers)**

Event Field Screens

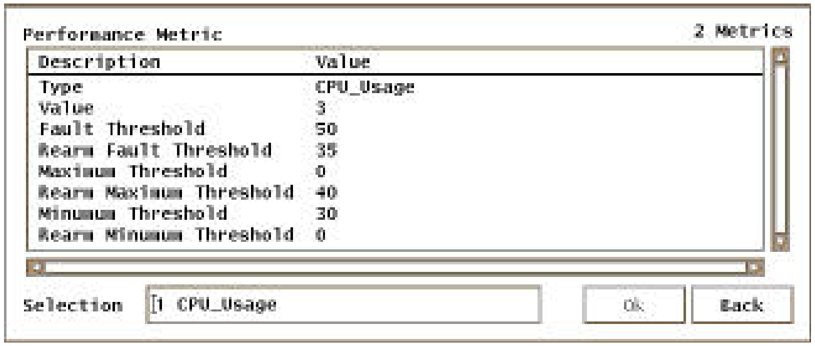


```
Host Information
Description              Value
Cell Name                /.../mssacell.hitc.com
Host Name                medusa.hitc.com
IP Address               155.157.99.34
OS Name                  SunOS
OS Major Version         5
OS Minor Version         4
OS Revision Level
OS Maintenance Level
```

```
Event Field
Description                 Value
Event ID                    0018605a-25f9-1158-bb03-8b9d6322aa77
Category                    Security Alert
Type                        Performance Threshold
SubType                     2
Mode                        2
Priority                    High
Time Stamp                  03/26/96 13:14:33
Sub System                  DMS
```

```
Tuple                                      1 Tuples
#  Type   Value
1  2      2

Selection
```



```
Performance Metric                              2 Metrics
Description                      Value
Type                             CPU_Usage
Value                            3
Fault Threshold                  50
Rearm Fault Threshold            35
Maximum Threshold                0
Rearm Maximum Threshold          40
Minumum Threshold                30
Rearm Minumum Threshold          0

Selection    1 CPU_Usage
```

Analysis/Troubleshooting: Hardware

- ECS hardware is COTS
- System troubleshooting principles apply
- HP OpenView for quick assessment of status
- MDA Event Log Browser for event sequence
- Initial troubleshooting
  - Review error message against hardware operator manual; prepare trouble ticket
  - Verify connections (power, network, interface cables)
  - Run internal systems and/or network diagnostics
  - Review system logs for evidence of previous problems
  - Attempt system reboot
  - If problem is hardware, report it to the DAAC Maintenance Coordinator

Hardware Problems: (Continued)

- **Difficult problems may require team attack by Maintenance Coordinator, System Administrator, and Network Administrator:**
  - **specific troubleshooting procedures described in COTS hardware manuals**
  - **non-replacement intervention (e.g., adjustment)**
  - **replace hardware with maintenance spare**
    - **locally purchased (non-stocked) item**
    - **installed spares (e.g., RAID storage, power supplies, network cards, tape drives)**

Hardware Problems: (Continued)

- If no resolution with local staff, maintenance support contractor may be called
  - Update trouble ticket with problem data, support provider data
  - Call technical support center
  - Facilitate site access by the technician
  - Update trouble ticket with data on the service call
  - If a part is replaced, additional data for trouble ticket
    - Part number of new item
    - Serial numbers (new and old)
    - Equipment Identification Number (EIN) of new item
    - Model number (Note: may require CCR)
    - Name of item replaced

Non-Standard Hardware Support

- For especially difficult cases, or if technical support is unsatisfactory
  - Escalation of the problem
    - Obtain attention of support contractor management
    - Call technical support center
  - Time and Material (T&M) Support
    - Last resort for mission-critical repairs

Preventive Maintenance

- **Only element that may require PM is the EMASS robot**
  - **Scheduled by local Maintenance Coordinator**
  - **Coordinated with maintenance organization and using organization**
    - **Scheduled to be performed by maintenance organization and to coincide with any corrective maintenance if possible**
    - **Scheduled to minimize operational impact**
  - **Documented using a trouble ticket**

Troubleshooting COTS Software

Issues

- Software use licenses
- Obtaining telephone assistance
- Obtaining software patches
- Obtaining software upgrades

Vendor support contracts

- First year warranty
- Subsequent years contracts
- Database at ILS office
- Contact ILS Logistics Engineer
  - E-mail: ilsmaint@ecs.hitc.com
  - Telephone: 1-800-ECS-DATA (327-3282)

COTS Software Licenses

Maintained in a property database by ECS Property Administrator

Major COTS Software License Restrictions

Software	Restriction
HP OpenView	One site license, unlimited users
AutoSys	Only one instance at a time may be active
ClearCase®	Five users concurrently
DDTS	Virtually unlimited (10,000 users)

COTS Software Installation

- COTS software is installed with any appropriate ECS customization
- Final Version Description Document (VDD) available
- Any residual media and commercial documentation should be protected (e.g., stored in locked cabinet, with access controlled by on-duty Operations Coordinator)

COTS Software Support

- Systematic initial troubleshooting
  - Software Event Browser (e.g., MDA Event Log Browser) to review event sequence
  - Review error messages, prepare Trouble Ticket (TT)
  - Review system logs for previous occurrences
  - Attempt software reload
  - Report to Maintenance Coordinator (forward TT)
- Additional troubleshooting
  - Procedures in COTS manuals
  - Vendor site on World Wide Web
  - Software diagnostics
  - Local procedures
  - Adjustment of tunable parameters

COTS Software Support (Cont.)

- Organize available data, update TT
  - Locate contact information for software vendor technical support center/help desk (telephone number, name, authorization code)
- Contact technical support center/help desk
  - Provide background data
  - Obtain case reference number
  - Update TT
  - Notify originator of the problem that help is initiated
- Coordinate with vendor and CM, update TT
  - Work with technical support center/help desk (e.g., troubleshooting, patch, work-around)
  - CCB authorization required for patch

COTS Software Support (Cont.)

- Escalation may be required
  - Lack of timely solution
  - Unsatisfactory performance of technical support center/ help desk
- Notify SEO
  - Senior Systems Engineers
  - ILS Logistics Engineer coordination for escalation within vendor organization

Troubleshooting of Custom Software

- Code maintained at ECS Development Facility
- ClearCase® for library storage and maintenance
- Sources of maintenance changes
  - ESDIS CCB directives
  - Site-level CCB directives
  - Developer modifications or upgrades
  - Trouble Tickets

Implementation of Modifications

- Responsible Engineer (RE) selected by each ECS organization
- SEO RE establishes set of CCRs for build
- Site/Center RE determines site-unique extensions
- System and center REs establish schedules for implementation, integration, and test
- SEO RE maintains CCR lists and schedule
- SEO RE maintains VDD
- RE or team for CCR obtains source code/files, implements change, performs programmer testing, updates documentation

Custom Software Support

- Science software maintenance not responsibility of ECS on-site maintenance engineers
- Sources of Trouble Tickets for custom software
  - Anomalies
  - Apparent incorrect execution by software
  - Inefficiencies
  - Sub-optimal use of system resources
  - TTs may be submitted by users, operators, customers, analysts, maintenance personnel, management
  - TTs capture supporting information and data on problem

Custom Software Support (Cont.)

- Troubleshooting is ad hoc, but systematic
- For problem caused by non-ECS element, TT and data are provided to maintainer at that element

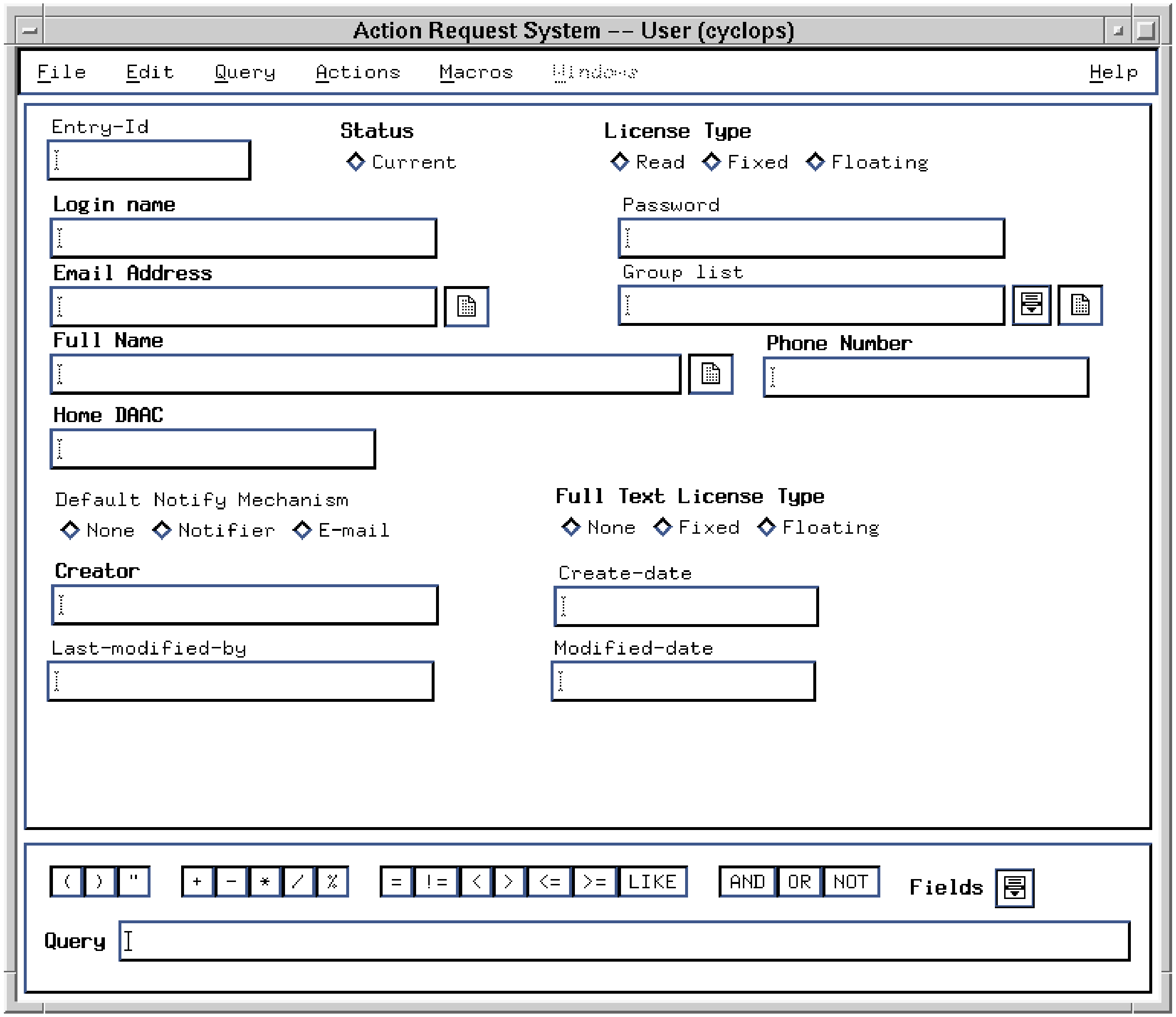
Trouble Ticket (TT)

- Documentation of system problems
- COTS Software (Remedy)
- Documentation of changes
- Failure Review Board
- Emergency fixes
- Configuration changes → CCR

Using Remedy

- Creating and viewing Trouble Tickets
- Adding users to Remedy — Database Administrator
- Controlling and changing privileges in Remedy — Configuration Management Administrator
- Modifying Remedy’s configuration — Configuration Management Administrator.
- Generating Trouble Ticket reports — System Administrator, others

Remedy RelB-User Schema Screen



Entry-Id

Status
◇ Current

License Type
◇ Read ◇ Fixed ◇ Floating

Login name

Password

Email Address

Group list

Full Name

Phone Number

Home DAAC

Default Notify Mechanism
◇ None ◇ Notifier ◇ E-mail

Full Text License Type
◇ None ◇ Fixed ◇ Floating

Creator

Create-date

Last-modified-by

Modified-date

Query

Adding Users to Remedy

- Status
- License Type
- Login Name
- Password
- Email Address
- Group List
- Full Name
- Phone Number
- Home DAAC
- Default Notify Mechanism
- Full Text License
- Creator

Changing Privileges in Remedy

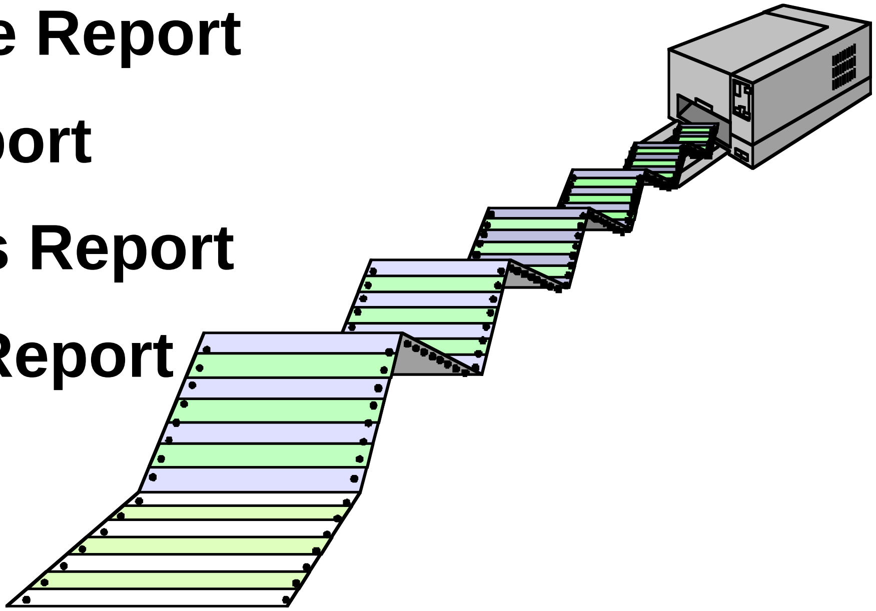
- Access privileges (for fields)
  - View
  - Change
- Privilege change methods
  - Change group assignment
  - Change privileges of a group
    - Use Admin tool to define group access for schemas (Remedy databases)

Changing Remedy Configuration

- Closing Codes (RelB-Menu-Closing Codes)
- Software Resources (RelB-Menu-Software Resources)
- Hardware Resources (RelB-Menu-Hardware Resources)
- Key Words (RelB-Menu-Key Words)
- Problem Type (RelB-Menu-Problem Type)
- Forward-to (RelB-TT-Sites)

Generating Trouble Ticket Reports

- Trouble Ticket Status Report (Summary)
- Trouble Ticket Status Report (Criteria)
- Trouble Ticket Status Report (SMC)
- Trouble Ticket Resource Report
- Trouble Ticket User Report
- Trouble Ticket Statistics Report
- Trouble Ticket Priority Report



Operational Work-around

- Managed by the ECS Operations Coordinator at each center
- Master list of work-arounds and associated trouble tickets and configuration change requests (CCRs) kept in either hard-copy or soft-copy form for the operations staff
- Hard-copy and soft-copy procedure documents are “red-lined” for use by the operations staff
- Work-arounds affecting multiple sites are coordinated by the ECS organizations and monitored by ECS M&O Office staff

Diagnosing Network Problems

- Network failures require same management as other failures
  - Detection of the fault
  - Isolation of the fault
  - Correction of the fault
- Standard troubleshooting tools apply
  - Error logs
  - Error detection processes
  - Diagnostic testing

Identifying Connectivity Problems

- HP OpenView -- color of connections on maps

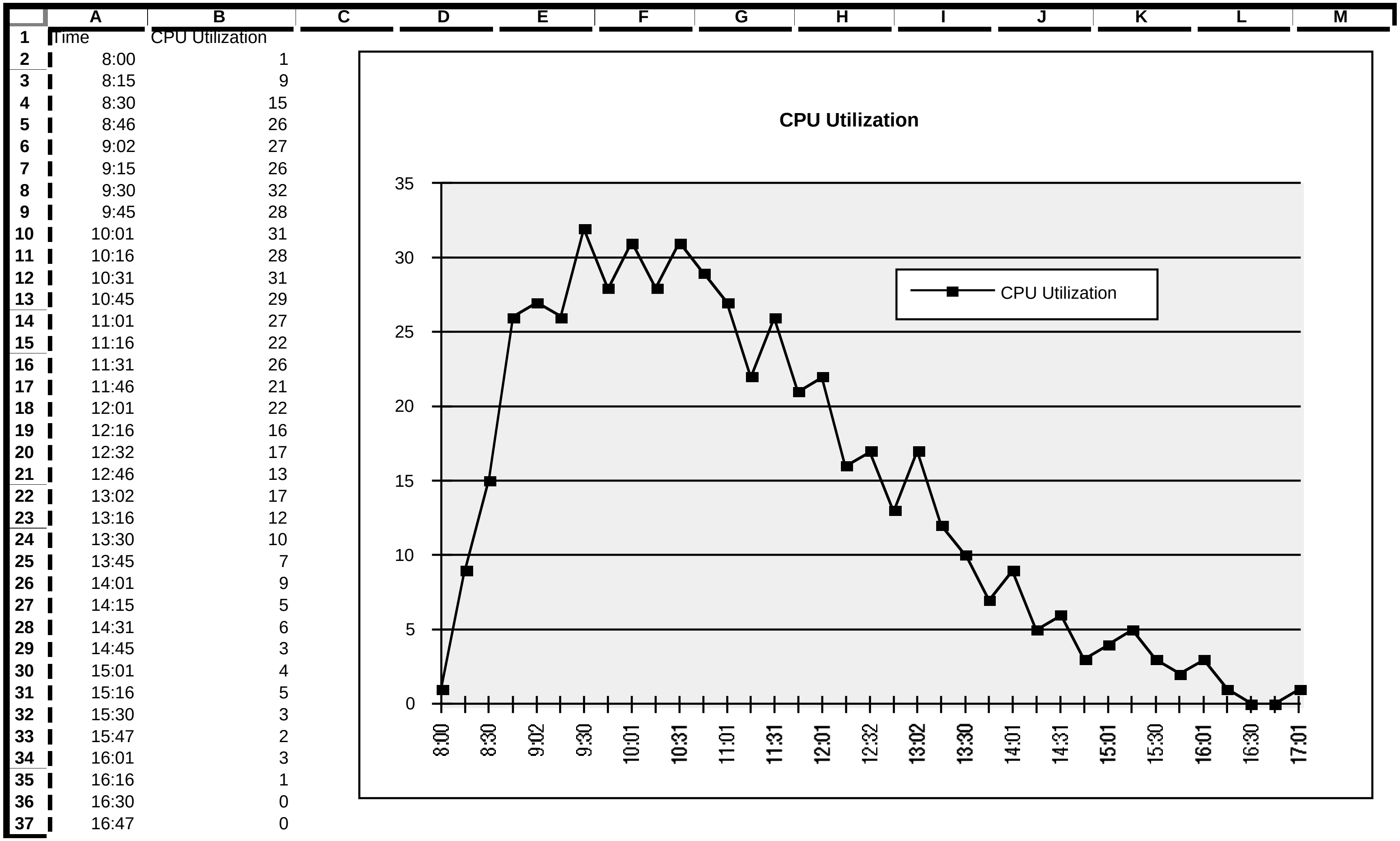
– cyan:	warning
– yellow:	minor
– orange:	major
– red:	critical

- HP OpenView Fault Diagnostic Aids
  - Ping
  - Remote Ping
  - Route Analysis

Diagnosing Performance Problems

- HP OpenView
  - Check interface traffic
  - Check CPU loading

Example of HP OpenView Graphical Display of CPU Usage



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Time	CPU Utilization											
2	8:00	1											
3	8:15	9											
4	8:30	15											
5	8:46	26											
6	9:02	27											
7	9:15	26											
8	9:30	32											
9	9:45	28											
10	10:01	31											
11	10:16	28											
12	10:31	31											
13	10:45	29											
14	11:01	27											
15	11:16	22											
16	11:31	26											
17	11:46	21											
18	12:01	22											
19	12:16	16											
20	12:32	17											
21	12:46	13											
22	13:02	17											
23	13:16	12											
24	13:30	10											
25	13:45	7											
26	14:01	9											
27	14:15	5											
28	14:31	6											
29	14:45	3											
30	15:01	4											
31	15:16	5											
32	15:30	3											
33	15:47	2											
34	16:01	3											
35	16:16	1											
36	16:30	0											
37	16:47	0											

Diagnosing Network Service Problems

- If unable to access a network service (e.g., ftp, telnet) on a remote system, use diagnostic procedure
- General Systematic Troubleshooting
  - Review Trouble Ticket
  - HP Open View
    - Look for color alerts
    - Locate relevant host
    - Check network activity, traffic on host
    - Check CPU load on host

Viewing Historical Trends

- HP OpenView Network Node Manager
  - Data collection
  - Event configuration
  - Application building
- Process
  - Establish baselines
  - Build applications to monitor trends
  - Establish and refine thresholds
  - Set up event-triggered actions

Viewing Historical Trends (Cont.)

- HP OpenView Grapher
  - Viewing of collected information in graph form
  - Graphing of combinations of data values
  - Viewing data values representing different instances of data variables or different variables for different nodes
  - Viewing data for selected nodes or viewing all the data in the Data Collector database

Viewing Historical Trends (Cont.)

Table 1
ECS MIB Data Collection Definitions

MIB Object Group	Resource/Expression
ICMP	ICMP%InErrors
	ICMP%InDestUnreachs
	ICMP%OutErrors
	ICMP%OutDestUnreachs
TCP	TCP%InErrors
UDP	UDP%InErrors
IP	IP%InHdrErrors
	IP%InAddrErrors
	IP%InUnknownProtos
	IP%InDiscards
	IP%OutDiscards
	IP%OutNoRoutes
Network Interface	If%InDiscards
	If%InErrors
	If%InUnknownProtos
	if%OutDiscards
	If%OutErrors

Viewing Historical Trends (Cont.)

- HP OpenView Event Log Browser
  - List events at or near the time of a problem